GP-2131

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

#4

APPLICANT(S):	Shinako Matsuyama, et al.	ATTY. DOCKET NO.	09792909-5002
SERIAL NO.	09/843,403	GROUP ART UNIT:	2131
DATE FILED:	April 26, 2001	EXAMINER:	

INVENTION: "ACCESS CONTROL SYSTEM, ACCESS CONTROL METHOD, DEVICE, ACCESS CONTROL SERVER, ACCESS-CONTROL-SERVER, REGISTRATION SERVER, DATA PROCESSING APPARATUS, AND PROGRAM STORAGE MEDIUM"

SUBMISSION OF CERTIFIED COPY OF PRIORITY DOCUMENT

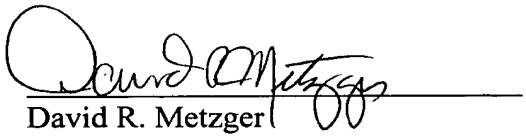
Assistant Commissioner of Patents
Washington, D.C. 20231

S I R:

Applicants herewith submit the certified copies of Japanese Applications Nos. P2000-125787 filed April 26, 2000, and P2001-089672 filed March 27,2 001, and claims priority to the April 26, 2000, date.

The Commissioner is authorized to charge any fees which may be due or credit any overpayments to Deposit Account No. 19-3140. A duplicate copy of this sheet is enclosed for that purpose.

Respectfully submitted,

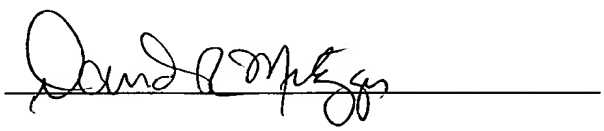


(Reg. No. 32,919

David R. Metzger
SONNENSCHEIN NATH & ROSENTHAL
P.O. Box #061080
Wacker Drive Station - Sears Tower
Chicago, Illinois 60606-1080
Telephone 312/876-8000
Customer #26263
Attorneys for Applicants

CERTIFICATE OF MAILING

I hereby certify that a true copy of the foregoing Submission of Certified Copies of Priority Documents was forwarded to the United States Patent Office via U.S. First Class mail on August 21, 2001.



S01P0625US00

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　４月２６日

出願番号
Application Number: 特願２０００－１２５７８７

出願人
Applicant (s): ソニー株式会社

２００１年　３月　９日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２００１－３０１６４３９

【書類名】　特許願

【整理番号】　00001536

【提出日】　平成12年 4月26日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 9/32

【発明の名称】　アクセス制御システムおよびアクセス制御方法、並びにプログラム提供媒体

【請求項の数】　26

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　松山　科子

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　石橋　義人

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　二村　一郎

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　昆　雅士

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　渡辺　秀明

【特許出願人】
【識別番号】　000002185
【氏名又は名称】　ソニー株式会社
【代表者】　出井　伸之
【代理人】
【識別番号】　100101801
【弁理士】
【氏名又は名称】　山田　英治
【電話番号】　03-5541-7577
【選任した代理人】
【識別番号】　100093241
【弁理士】
【氏名又は名称】　宮田　正昭
【電話番号】　03-5541-7577
【選任した代理人】
【識別番号】　100086531
【弁理士】
【氏名又は名称】　澤田　俊夫
【電話番号】　03-5541-7577
【手数料の表示】
【予納台帳番号】　062721
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9904833
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　アクセス制御システムおよびアクセス制御方法、並びにプログラム提供媒体

【特許請求の範囲】

【請求項１】

公開鍵証明書発行局が認証対象に発行する公開鍵証明書を利用して公開鍵系暗号方式を使用したデータ転送を行なうデータ転送システムにおけるアクセス制御システムにおいて、

前記認証対象であり、サービスを提供するサービスプロバイダと、

前記認証対象であり、前記サービスプロバイダの提供するサービスを受領するサービス受領デバイスと、

前記サービス受領デバイスのアクセスが許可されたサービスプロバイダを識別可能なアクセス許可書を前記サービス受領デバイスに対して発行するアクセス制御サーバと、を有し、

前記サービス提供プロバイダは、前記サービス受領デバイスからのアクセス要求に対するアクセス許可判定を、前記アクセス許可書に基づいて実行する構成であることを特徴とするアクセス制御システム。

【請求項２】

前記アクセス制御システムは、さらに、

アクセス制御サーバ登録サーバを有し、

前記アクセス制御サーバ登録サーバは、前記サービス受領デバイスからのアクセス許可書発行要求を受領して、前記アクセス制御サーバに対するアクセス許可書発行処理の実行要求を行なう構成であることを特徴とする請求項１に記載のアクセス制御システム。

【請求項３】

前記アクセス制御システムは、さらに、

ユーザ端末によって利用可能なコンテンツまたはサービスの提供を可能とするコンテンツまたはサービスの流通インフラを提供または管理する機関であるシステムホルダを有し、

前記システムホルダは、前記サービスプロバイダおよびサービス受領デバイスを管轄し、認証対象とした構成であることを特徴とする請求項１に記載のアクセス制御システム。

【請求項４】

前記アクセス制御サーバは、前記システムホルダ各々に対応して設けられ、

前記システムホルダの管轄するサービスプロバイダの提供するサービスに関するアクセス許可書を発行する構成であることを特徴とする請求項３に記載のアクセス制御システム。

【請求項５】

前記アクセス制御サーバは、前記システムホルダの複数に対して共通に設けられ、

該複数のシステムホルダの管轄するサービスプロバイダの提供するサービスに関するアクセス許可書を発行する構成であることを特徴とする請求項３に記載のアクセス制御システム。

【請求項６】

前記アクセス制御システムは、さらに、

前記システムホルダを管轄するルート登録局を有し、

前記ルート登録局は、前記システムホルダからの要求に基づいて該ルート登録局の管轄する認証対象の公開鍵証明書の発行要求を前記公開鍵証明書発行局に対して実行する構成であることを特徴とする請求項３に記載のアクセス制御システム。

【請求項７】

前記アクセス制御サーバは、

前記アクセス許可書を、サービスプロバイダ毎に独立に使用可能な態様で生成することを特徴とする請求項１に記載のアクセス制御システム。

【請求項８】

前記アクセス制御サーバは、

前記アクセス許可書を、複数のサービスプロバイダに共通に使用可能な態様で生成することを特徴とする請求項１に記載のアクセス制御システム。

【請求項９】

前記アクセス制御サーバは、

前記アクセス制御サーバの設定するアクセス制御サーバ設定固定フィールドと

前記サービスプロバイダの各々が設定するサービスプロバイダ設定オプションフィールドと、

前記アクセス制御サーバによる電子署名フィールドと、

から成るフォーマットで、前記アクセス許可書を生成する構成であることを特徴とする請求項１に記載のアクセス制御システム。

【請求項１０】

前記サービスプロバイダ設定オプションフィールドには、サービス受領デバイス毎のアクセス可否を決定する識別データを含み、該識別データは、前記サービス受領デバイスのユーザに関する個人情報、ユーザＩＤ，ユーザデバイスＩＤ，またはアクセス許可識別フラグの少なくともいずれかを含む構成であることを特徴とする請求項９に記載のアクセス制御システム。

【請求項１１】

前記サービスプロバイダ、前記サービス受領デバイス、前記アクセス制御サーバ間において、直接あるいは仲介手段を介して実行されるデータ転送は、データ転送相互間における相互認証処理が実行され、相互認証が成立したことを条件としたデータ転送として実行する構成であることを特徴とする請求項１に記載のアクセス制御システム。

【請求項１２】

前記サービスプロバイダ、前記サービス受領デバイス、前記アクセス制御サーバ間において、直接あるいは仲介手段を介して実行される転送データはデータ送信側の電子署名が付加されたデータとして転送する構成であることを特徴とする請求項１に記載のアクセス制御システム。

【請求項１３】

前記サービスプロバイタは、

サービスを提供するデバイスであることを特徴とする請求項１に記載のアクセ

ス制御システム。

【請求項１４】

前記アクセス制御サーバは、

前記アクセス許可書に設定されたアクセス許可を取り消すアクセス許可書の変更処理を実行する構成であることを特徴とする請求項１に記載のアクセス制御システム。

【請求項１５】

公開鍵証明書発行局が認証対象に発行する公開鍵証明書を利用して公開鍵系暗号方式を使用したデータ転送を行なうデータ転送システムにおけるアクセス制御方法であり、

サービス提供プロバイダにおいて、サービス受領デバイスから、サービス制御サーバの発行したアクセス許可書を受領するステップと、

前記アクセス許可書に基づいて、前記サービス受領デバイスのアクセス要求に対するアクセス許可判定を実行するステップと、

を有することを特徴とするアクセス制御方法。

【請求項１６】

前記アクセス制御方法は、さらに、

アクセス制御サーバにおいて、サービス受領デバイスのアクセスが許可されたサービスプロバイダを識別可能なアクセス許可書をサービス受領デバイスに対して発行するアクセス許可書発行ステップと、

を含むことを特徴とする請求項１５に記載のアクセス制御方法。

【請求項１７】

前記アクセス制御方法は、さらに、

前記アクセス制御サーバ登録サーバにおいて、前記サービス受領デバイスからのアクセス許可書発行要求を受領して、前記アクセス制御サーバに対するアクセス許可書発行処理の実行要求を行なうステップを有することを特徴とする請求項１５に記載のアクセス制御方法。

【請求項１８】

前記アクセス許可書発行ステップは、

ユーザ端末によって利用可能なコンテンツまたはサービスの提供を可能とするコンテンツまたはサービスの流通インフラを提供または管理する機関であるシステムホルダの管轄するサービスプロバイダからの発行要求に基づいて実行されることを特徴とする請求項１５に記載のアクセス制御方法。

【請求項１９】

前記アクセス許可書発行ステップは、

サービスプロバイダ毎に独立に使用可能な態様で前記アクセス許可書を生成することを特徴とする請求項１５に記載のアクセス制御方法。

【請求項２０】

前記アクセス許可書発行ステップは、

複数のサービスプロバイダに共通に使用可能な態様で前記アクセス許可書を生成することを特徴とする請求項１５に記載のアクセス制御方法。

【請求項２１】

前記アクセス許可書発行ステップは、

前記アクセス制御サーバの設定するアクセス制御サーバ設定固定フィールドと、

前記サービスプロバイダの各々が設定するサービスプロバイダ設定オプションフィールドと、

前記アクセス制御サーバによる電子署名フィールドと、

から成るフォーマットで生成することを特徴とする請求項１５に記載のアクセス制御方法。

【請求項２２】

前記サービスプロバイダにおいて実行されるアクセス許可判定実行ステップは、

前記アクセス許可書に含まれるサービス受領デバイス毎のアクセス可否を決定する識別データとしての前記サービス受領デバイスのユーザに関する個人情報、ユーザＩＤ，ユーザデバイスＩＤ，またはアクセス許可識別フラグの少なくともいずれかに基づいてアクセス許可の判定を実行することを特徴とする請求項１５に記載のアクセス制御方法。

【請求項２３】

前記サービスプロバイダ、前記サービス受領デバイス、前記アクセス制御サーバ間において、直接あるいは仲介手段を介して実行されるデータ転送は、データ転送相互間における相互認証処理を実行し、相互認証が成立したことを条件としたデータ転送として実行することを特徴とする請求項１５に記載のアクセス制御方法。

【請求項２４】

前記サービスプロバイダ、前記サービス受領デバイス、前記アクセス制御サーバ間において、直接あるいは仲介手段を介して実行される転送データにはデータ送信側の電子署名を付加することを特徴とする請求項１５に記載のアクセス制御方法。

【請求項２５】

前記アクセス制御方法は、さらに、

前記アクセス制御サーバにおいて、

前記アクセス許可書に設定されたアクセス許可を取り消すアクセス許可書の変更処理を実行するアクセス許可書変更処理ステップを含むことを特徴とする請求項１５に記載のアクセス制御方法。

【請求項２６】

公開鍵証明書発行局が認証対象に発行する公開鍵証明書を利用して公開鍵系暗号方式を使用したデータ転送を行なうデータ転送システムにおけるアクセス制御処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

サービス提供プロバイダにおいて、サービス受領デバイスから、サービス制御サーバの発行したアクセス許可書を受領するステップと、

前記アクセス許可書に基づいて、前記サービス受領デバイスのアクセス要求に対するアクセス許可判定を実行するステップと、

を有することを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はアクセス制御システムおよびアクセス制御方法に関する。特に、様々なサービスプロバイダが提供するサービスへのユーザデバイスからのアクセスに対する制御を行なうアクセス制御システムおよびアクセス制御方法に関する。さらに、詳細には、各エンティテイが公開鍵証明書を保有し、公開鍵ベースの相互認証を実行して、データ通信を実行するシステムにおいて有用な、アクセス制御システムおよびアクセス制御方法に関するものである。

【０００２】

【従来の技術】

昨今、ゲームプログラム、音声データ、画像データ、文書作成プログラム等、様々なソフトウエアデータ（以下、これらをコンテンツ（Content）と呼ぶ）が、インターネット等のネットワークを介して流通している。また、オンラインショッピング等、ネットワークを介した商品売買も次第に盛んになってきている。

【０００３】

このようなネットワークを介したデータ通信においては、データ送信側とデータ受信側とが互いに正規なデータ送受信対象であることを確認した上で、必要な情報を転送する、すなわちセキュリティを考慮したデータ転送構成をとるのが一般的となっている。データ転送の際のセキュリティ構成を実現する１つの手法が、転送データの暗号化処理、データに対する署名処理である。

【０００４】

暗号化データは、所定の手続きによる復号化処理によって利用可能な復号データ（平文）に戻すことができる。このような情報の暗号化処理に暗号化鍵を用い、復号化処理に復号化鍵を用いるデータ暗号化、復号化方法は従来からよく知られている。

【０００５】

暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類あるが、その１つの例としていわゆる公開鍵暗号方式と呼ばれる方式がある。公開鍵暗号方式は、発信者と受信者の鍵を異なるものとして、一方の鍵を不特定のユーザが使用可能な公開鍵として、他方を秘密に保つ秘密鍵とするものである。

例えば、データ暗号化鍵を公開鍵とし、復号鍵を秘密鍵とする。あるいは、認証子生成鍵を秘密鍵とし、認証子復号鍵を公開鍵とする等の態様において使用される。

【０００６】

暗号化、復号化に共通の鍵を用いるいわゆる共通鍵暗号化方式と異なり、公開鍵暗号方式では秘密に保つ必要のある秘密鍵は、特定の１人が持てばよいため鍵の管理において有利である。ただし、公開鍵暗号方式は共通鍵暗号化方式に比較してデータ処理速度が遅く、秘密鍵の配送、ディジタル署名等のデータ量の少ない対象に多く用いられている。公開鍵暗号方式の代表的なものにはＲＳＡ（Rivest-Shamir-Adleman）暗号がある。これは非常に大きな２つの素数（例えば１５０桁）の積を用いるものであり、大きな２つの素数（例えば１５０桁）の積の素因数分解する処理の困難さを利用している。

【０００７】

公開鍵暗号方式では、不特定多数に公開鍵を使用可能とする構成であり、配布する公開鍵が正当なものであるか否かを証明する証明書、いわゆる公開鍵証明書を使用する方法が多く用いられている。例えば、利用者Ａが公開鍵、秘密鍵のペアを生成して、生成した公開鍵を認証局に対して送付して公開鍵証明書を認証局から入手する。利用者Ａは公開鍵証明書を一般に公開する。不特定のユーザは公開鍵証明書から所定の手続きを経て公開鍵を入手して文書等を暗号化して利用者Ａに送付する。利用者Ａは秘密鍵を用いて暗号化文書等を復号する等のシステムである。また、利用者Ａは、秘密鍵を用いて文書等に署名を付け、不特定のユーザが公開鍵証明書から所定の手続きを経て公開鍵を入手して、その署名の検証を行なうシステムである。

【０００８】

公開鍵証明書について図１を用いて説明する。公開鍵証明書は、公開鍵暗号方式における認証局（ＣＡ：Certificate AuthorityまたはＩＡ：Issuer Authority）が発行する証明書であり、ユーザが自己のＩＤ、公開鍵等を認証局に提出することにより、認証局側が認証局のＩＤや有効期限等の情報を付加し、さらに認証局による署名を付加して作成される証明書である。

【０００９】

図１に示す公開鍵証明書は、証明書のバージョン番号、認証局（ＩＡ）が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前（ユーザＩＤ）、証明書利用者の公開鍵並びに電子署名を含む。

【００１０】

電子署名は、証明書のバージョン番号、認証局が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前並びに証明書利用者の公開鍵全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して認証局の秘密鍵を用いて生成したデータである。

【００１１】

認証局は、図１に示す公開鍵証明書を発行するとともに、有効期限が切れた公開鍵証明書を更新し、不正を行った利用者の排斥を行うための不正者リストの作成、管理、配布（これをリボケーション：Revocationと呼ぶ）を行う。また、必要に応じて公開鍵・秘密鍵の生成も行う。

【００１２】

一方、この公開鍵証明書を利用する際には、利用者は自己が保持する認証局の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の認証局の公開鍵を保持している必要がある。

【００１３】

【発明が解決しようとする課題】

上述のような認証局発行の公開鍵証明書を用いた公開鍵暗号方式によるデータ送信システムにおいては、使用する公開鍵が異なれば、その公開鍵に対して新たに認証局に対して公開鍵証明書の発行を依頼、あるいは認証局構成を持つ認証システムを構築することが必要となる。すなわち、例えばコンテンツの配信、商品提供サービスを行なうサービスプロバイダは、新たなサービス（新たな電子配信

システム）を開始し、新たな公開鍵の使用を開始する際に、逐一、新たな公開鍵に対応する公開鍵証明書の発行、管理を認証局に依頼、あるいは、新たに認証局構成を持つ認証システムを構築しなければならず、多大なコスト、時間を要するという問題があった。

【００１４】

また、異なるサービスを提供する複数の異なるサービスプロバイダの提供するサービスを１つのユーザデバイスが受けようとする場合、ユーザデバイス側では、各サービスプロバイダが設定した独自の仕様、アプリケーションに従った設定を、個々のサービス毎に実行することが必要であった。また、サービスプロバイダ側でも、それぞれ独自にユーザ情報をユーサデバイスを介して受領し、独自に管理、審査を実行して自身の提供するサービスに対する許可または拒否等の判定を実行することが必要とっなっている。

【００１５】

例えば、ユーザデバイスが新たなサービスプロバイダの提供する新たなサービスを開始したい場合には、そのサービスプロバイダの要求する項目に従ったユーザデータ、端末データ等をサービスプロバイダに送信し、サービスプロバイダはユーザデバイスからのデータに基づいて、ユーザを登録しサービスを開始していた。

【００１６】

このように、サービス毎に独自のユーザ管理、アクセス制御を行なうことは、サービスプロバイダ、ユーザ双方にとって負担であり、また、双方のデバイスにおいて、様々な登録用のデータを格納、管理することが要求されることになり、デバイス自体の負担も増加することになる。

【００１７】

本発明は、このような点に鑑みてなされたものであり、様々なサービスプロバイダが提供するサービスへのユーザデバイスからのアクセスに対する制御をサービスプロバイダ個々が独自に実行することが要求されないアクセス制御システムおよびアクセス制御方法を実現することを目的とする。

【００１８】

【課題を解決するための手段】

本発明の第１の側面は、

公開鍵証明書発行局が認証対象に発行する公開鍵証明書を利用して公開鍵系暗号方式を使用したデータ転送を行なうデータ転送システムにおけるアクセス制御システムにおいて、

前記認証対象であり、サービスを提供するサービスプロバイダと、

前記認証対象であり、前記サービスプロバイダの提供するサービスを受領するサービス受領デバイスと、

前記サービス受領デバイスのアクセスが許可されたサービスプロバイダを識別可能なアクセス許可書を前記サービス受領デバイスに対して発行するアクセス制御サーバとを有し、

前記サービス提供プロバイダは、前記サービス受領デバイスからのアクセス要求に対するアクセス許可判定を、前記アクセス許可書に基づいて実行する構成であることを特徴とするアクセス制御システムにある。

【００１９】

さらに、本発明のアクセス制御システムの一実施態様において、アクセス制御サーバ登録サーバを有し、前記アクセス制御サーバ登録サーバは、前記サービス受領デバイスからのアクセス許可書発行要求を受領して、前記アクセス制御サーバに対するアクセス許可書発行処理の実行要求を行なう構成であることを特徴とする。

【００２０】

さらに、本発明のアクセス制御システムの一実施態様において、ユーザ端末によって利用可能なコンテンツまたはサービスの提供を可能とするコンテンツまたはサービスの流通インフラを提供または管理する機関であるシステムホルダを有し、前記システムホルダは、前記サービスプロバイダおよびサービス受領デバイスを管轄し、認証対象とした構成であることを特徴とする。

【００２１】

さらに、本発明のアクセス制御システムの一実施態様において、前記アクセス制御サーバは、前記システムホルダ各々に対応して設けられ、前記システムホル

ダの管轄するサービスプロバイダの提供するサービスに関するアクセス許可書を発行する構成であることを特徴とする。

【００２２】

さらに、本発明のアクセス制御システムの一実施態様において、前記アクセス制御サーバは、前記システムホルダの複数に対して共通に設けられ、該複数のシステムホルダの管轄するサービスプロバイダの提供するサービスに関するアクセス許可書を発行する構成であることを特徴とする。

【００２３】

さらに、本発明のアクセス制御システムの一実施態様において、前記システムホルダを管轄するルート登録局を有し、前記ルート登録局は、前記システムホルダからの要求に基づいて該ルート登録局の管轄する認証対象の公開鍵証明書の発行要求を前記公開鍵証明書発行局に対して実行する構成であることを特徴とする。

【００２４】

さらに、本発明のアクセス制御システムの一実施態様において、前記アクセス制御サーバは、前記アクセス許可書を、サービスプロバイダ毎に独立に使用可能な態様で生成することを特徴とする。

【００２５】

さらに、本発明のアクセス制御システムの一実施態様において、前記アクセス制御サーバは、前記アクセス許可書を、複数のサービスプロバイダに共通に使用可能な態様で生成することを特徴とする。

【００２６】

さらに、本発明のアクセス制御システムの一実施態様において、前記アクセス制御サーバは、前記アクセス制御サーバの設定するアクセス制御サーバ設定固定フィールドと、前記サービスプロバイダの各々が設定するサービスプロバイダ設定オプションフィールドと、

前記アクセス制御サーバによる電子署名フィールドと、から成るフォーマットで、前記アクセス許可書を生成する構成であることを特徴とする。

【００２７】

さらに、本発明のアクセス制御システムの一実施態様において、前記サービスプロバイダ設定オプションフィールドには、サービス受領デバイス毎のアクセス可否を決定する識別データを含み、該識別データは、前記サービス受領デバイスのユーザに関する個人情報、ユーザＩＤ，ユーザデバイスＩＤ，またはアクセス許可識別フラグの少なくともいずれかを含む構成であることを特徴とする。

【００２８】

さらに、本発明のアクセス制御システムの一実施態様において、前記サービスプロバイダ、前記サービス受領デバイス、前記アクセス制御サーバ間において、直接あるいは仲介手段を介して実行されるデータ転送は、データ転送相互間における相互認証処理が実行され、相互認証が成立したことを条件としたデータ転送として実行する構成であることを特徴とする。

【００２９】

さらに、本発明のアクセス制御システムの一実施態様において、前記サービスプロバイダ、前記サービス受領デバイス、前記アクセス制御サーバ間において、直接あるいは仲介手段を介して実行される転送データはデータ送信側の電子署名が付加されたデータとして転送する構成であることを特徴とする。

【００３０】

さらに、本発明のアクセス制御システムの一実施態様において、前記サービスプロバイタは、サービスを提供するデバイスであることを特徴とする。

【００３１】

さらに、本発明のアクセス制御システムの一実施態様において、前記アクセス制御サーバは、前記アクセス許可書に設定されたアクセス許可を取り消すアクセス許可書の変更処理を実行する構成であることを特徴とする。

【００３２】

さらに、本発明の第２の側面は、

公開鍵証明書発行局が認証対象に発行する公開鍵証明書を利用して公開鍵系暗号方式を使用したデータ転送を行なうデータ転送システムにおけるアクセス制御方法であり、

サービス提供プロバイダにおいて、サービス受領デバイスから、サービス制御

サーバの発行したアクセス許可書を受領するステップと、

前記アクセス許可書に基づいて、前記サービス受領デバイスのアクセス要求に対するアクセス許可判定を実行するステップと、

を有することを特徴とするアクセス制御方法にある。

【００３３】

さらに、本発明のアクセス制御方法の一実施態様において、アクセス制御サーバにおいて、サービス受領デバイスのアクセスが許可されたサービスプロバイダを識別可能なアクセス許可書をサービス受領デバイスに対して発行するアクセス許可書発行ステップとを含むことを特徴とする。

【００３４】

さらに、本発明のアクセス制御方法の一実施態様において、前記アクセス制御サーバ登録サーバにおいて、前記サービス受領デバイスからのアクセス許可書発行要求を受領して、前記アクセス制御サーバに対するアクセス許可書発行処理の実行要求を行なうステップを有することを特徴とする。

【００３５】

さらに、本発明のアクセス制御方法の一実施態様において、前記アクセス許可書発行ステップは、ユーザ端末によって利用可能なコンテンツまたはサービスの提供を可能とするコンテンツまたはサービスの流通インフラを提供または管理する機関であるシステムホルダの管轄するサービスプロバイダからの発行要求に基づいて実行されることを特徴とする。

【００３６】

さらに、本発明のアクセス制御方法の一実施態様において、前記アクセス許可書発行ステップは、サービスプロバイダ毎に独立に使用可能な態様で前記アクセス許可書を生成することを特徴とする。

【００３７】

さらに、本発明のアクセス制御方法の一実施態様において、前記アクセス許可書発行ステップは、複数のサービスプロバイダに共通に使用可能な態様で前記アクセス許可書を生成することを特徴とする。

【００３８】

さらに、本発明のアクセス制御方法の一実施態様において、前記アクセス許可書発行ステップは、前記アクセス制御サーバの設定するアクセス制御サーバ設定固定フィールドと、前記サービスプロバイダの各々が設定するサービスプロバイダ設定オプションフィールドと、前記アクセス制御サーバによる電子署名フィールドと、から成るフォーマットで生成することを特徴とする。

【００３９】

さらに、本発明のアクセス制御方法の一実施態様において、前記サービスプロバイダにおいて実行されるアクセス許可判定実行ステップは、前記アクセス許可書に含まれるサービス受領デバイス毎のアクセス可否を決定する識別データとしての前記サービス受領デバイスのユーザに関する個人情報、ユーザＩＤ，ユーザデバイスＩＤ，またはアクセス許可識別フラグの少なくともいずれかに基づいてアクセス許可の判定を実行することを特徴とする。

【００４０】

さらに、本発明のアクセス制御方法の一実施態様において、前記サービスプロバイダ、前記サービス受領デバイス、前記アクセス制御サーバ間において、直接あるいは仲介手段を介して実行されるデータ転送は、データ転送相互間における相互認証処理を実行し、相互認証が成立したことを条件としたデータ転送として実行することを特徴とする。

【００４１】

さらに、本発明のアクセス制御方法の一実施態様において、前記サービスプロバイダ、前記サービス受領デバイス、前記アクセス制御サーバ間において、直接あるいは仲介手段を介して実行される転送データにはデータ送信側の電子署名を付加することを特徴とする。

【００４２】

さらに、本発明のアクセス制御方法の一実施態様において、前記アクセス制御サーバにおいて、前記アクセス許可書に設定されたアクセス許可を取り消すアクセス許可書の変更処理を実行するアクセス許可書変更処理ステップを含むことを特徴とする。

【００４３】

さらに、本発明の第３の側面は、

公開鍵証明書発行局が認証対象に発行する公開鍵証明書を利用して公開鍵系暗号方式を使用したデータ転送を行なうデータ転送システムにおけるアクセス制御処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

サービス提供プロバイダにおいて、サービス受領デバイスから、サービス制御サーバの発行したアクセス許可書を受領するステップと、

前記アクセス許可書に基づいて、前記サービス受領デバイスのアクセス要求に対するアクセス許可判定を実行するステップと、

を有することを特徴とするプログラム提供媒体にある。

【００４４】

本発明の第３の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、ＣＤやＦＤ、ＭＯなどの記憶媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【００４５】

このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【００４６】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００４７】

【発明の実施の形態】

以下、図面を参照しながら、本発明の実施の形態について詳細に説明する。

【００４８】

【実施例】

［階層構成を持つデータ配信システム概要］

まず、図２を用いて、本発明のアクセス制御システムおよびアクセス制御方法を実行可能なデータ通信システムのシステム構成例を説明する。図２のシステムは、公開鍵系暗号を使用したデータ通信システム構成例である。

【００４９】

図２において、ショップ２０６、端末２０７、ユーザデバイス２０８、ユーザの決済機関２０９が認証対象者、すなわち公開鍵暗号化方式によるデータ送受信を実行する主体となる。図２では、代表的な認証対象者としてショップ２０６、端末２０７、ユーザデバイス２０８、ユーザの決済機関２０９をそれぞれ１つづつ示しているが、これらは一般に多数存在し、また、これら以外にも様々な種類の認証対象者が存在することができる。

【００５０】

各々の登録局（ＲＡ）の管轄下にある認証対象者のショップ２０６、端末２０７、ユーザデバイス２０８、ユーザの決済機関２０９は、登録局（サービスプロバイダＲＡ）２０３、２０４、登録局（ペイメントＲＡ）２０５に対して、自己の使用する公開鍵に対応する公開鍵証明書の発行を要求する。

【００５１】

登録局（ＲＡ：Registration Authority）２０３、２０４、２０５は、各サービスにおける対象（サービスに参加するエンティティ、機器）を認証、あるいはそのサービスへの参加者の支払者を認証する（支払に対する保証）。また、登録局２０３、２０４、２０５は、各サービスにおける対象（サービスに参加するエンティティ、機器、ユーザ）の使用する公開鍵の公開鍵証明書発行要求を受領し、これをルート登録局（ルートＲＡ）２０２を介して公開鍵証明書発行局（ＩＡ）２０１に転送する。ルート登録局（ルートＲＡ）２０２は、認証済みの登録局２０３、２０４、２０５からの公開鍵証明書発行要求を受理する。すなわち、ルート登録局（ルートＲＡ）２０２が公開鍵証明書発行要求を受領するのは、ルート登録局（ルートＲＡ）２０２によって認証された登録局からの要求のみである

【００５２】

図２において、例えば登録局（サービスプロバイダＲＡ）２０３，２０４は音楽データ、画像データ、ゲームプログラム等のコンテンツ配信のサービス提供を実行するサービスプロバイダであり、登録局（ペイメントＲＡ）２０５は、銀行等のユーザの決済機関２０９とデータ送受信を行ない、ユーザの電子マネーの決済処理を実行するクリアリングセンタである。これら、登録局（ＲＡ）についても図２に示すものは一例であり、この他にも様々なサービスを提供する各種の登録局（ＲＡ）が存在可能である。

【００５３】

登録局（ＲＡ）は各サービス（システム）毎に存在し、その登録局（ＲＡ）を統括して認証するものとしてルートＲＡ（Root Registration Authority）２０２が存在する。ルートＲＡ（Root RA）２０２は次に述べるＩＡによって認証される。登録局（ＲＡ）２０３、２０４、２０５は、小規模なサービス主体であり、サービス提供者が独自のＲＡを持たない場合にはルートＲＡ（Root RA）２０２が機能を代行する事ができる。

【００５４】

図２に示すＩＡ，２０１は公開鍵証明書発行局（ＩＡ：Issuer Authority）である。ルート登録局（ルートＲＡ）２０２、または登録局（ＲＡ）２０３～２０５との間で相互認証を行い、ルートＲＡ２０２、または登録局（ＲＡ）２０３～２０５から渡される公開鍵証明書発行要求主体である対象を識別する対象識別子（ＩＤ）、対象の公開鍵、その他の公開鍵証明書に書き込む情報を元に公開鍵証明書を作成して登録局（ＲＡ）２０３～２０５に配布する。

【００５５】

公開鍵証明書発行局（ＩＡ）２０１に対して証明書発行を要求するルート登録局（ルートＲＡ）２０２、または登録局（ＲＡ）２０３～２０５は、公開鍵証明書発行局から認証されていることが条件となる。

【００５６】

また、公開鍵証明書発行局（ＩＡ）２０１は、ルート登録局（ルートＲＡ）２

０２、または登録局（ＲＡ）２０３～２０５の要求を受けて、公開鍵証明書の更新、無効化、削除あるいは対象者からの有効性確認に対する応答処理を行う。この公開鍵証明書発行局（ＩＡ：Issuer Authority）２０１は適切な法的機関の認定を受ける位置づけのものであり、その認可を持って認証されているものとする。

【００５７】

[システムホルダを構成要素としたデータ配信構成]

次に、上述のルート登録局（ルートＲＡ）と登録局（ＲＡ）との階層構成において、登録局（ＲＡ）をシステムホルダ（ＳＨ）として設定した構成例について説明する。

【００５８】

システムホルダ（ＳＨ）は、例えばインターネット上で展開するインターネットショップマーケットを主催、管理する機関、携帯電話の通信インフラを提供する機関、ケーブルテレビのケーブル使用を管理する機関、電子マネー・カード発行主体等によって構成される。すなわち、システムホルダは、様々なコンテンツ、サービスを提供可能とするコンテンツまたはサービスの流通インフラを提供、管理する機関として定義される。

【００５９】

図３にシステムホルダ３０１、コンテンツクリエイタ３０２、サービスプロバイダ３０３、ユーザ３０４の関係図を示し、図４にシステムホルダ、コンテンツクリエイタ、サービスプロバイダ、ユーザデバイスの具体例を示す。

【００６０】

図３において、システムホルダ３０１は、コンテンツクリエイタ３０２および、サービスプロバイダ３０３、ユーザ（デバイス）３０４において利用可能なコンテンツまたはサービス流通インフラを提供する。コンテンツクリエイタ３０２および、サービスプロバイダ３０３は、システムホルダ３０１の提供するインフラを利用してコンテンツの提供あるいはサービスの提供を行なう。ユーザ（デバイス）３０４は、システムホルダ３０１の提供するインフラを利用してサービスプロバイダ３０３の提供するサービスを受ける。

【００６１】

図４に、具体的なシステムホルダ、コンテンツクリエイタ、サービスプロバイダ、ユーザデバイスの例を示す。図４に示すように、例えば、システムホルダ（ＳＨ）が、インターネットショップマーケットを主催、管理する機関である場合、コンテンツクリエイタ（ＣＣ）は、インターネットショップマーケットに提供される商品を提供する。サービスプロバイダ（ＳＰ）は、提供された商品をインターネットショップにおいて販売するショップ（店）であり、ユーザデバイスは、インターネットショップを利用するＰＣ等である。

【００６２】

また、システムホルダ（ＳＨ）が、通信会社等、携帯電話通信インフラの提供機関である場合、コンテンツクリエイタ（ＣＣ）は、携帯電話の通信インフラを利用して提供可能なコンテンツ、商品を作成、製造する。サービスプロバイダ（ＳＰ）は、コンテンツクリエイタ（ＣＣ）から提供されるコンテンツ、商品を携帯電話の通信インフラを利用してユーザに対して販売、提供する。この場合のユーザデバイスは、携帯電話となる。

【００６３】

また、システムホルダ（ＳＨ）が、ケーブルテレビのケーブル通信管理会社等、ケーブルテレビ通信インフラの提供機関である場合、コンテンツクリエイタ（ＣＣ）は、ケーブルテレビの通信インフラを利用して提供可能なコンテンツ、商品を作成、製造する。ケーブルテレビに提供される番組もコンテンツに含まれる。サービスプロバイダ（ＳＰ）は、コンテンツクリエイタ（ＣＣ）から提供されるコンテンツ、商品をケーブルテレビの通信インフラを利用してユーザに対して販売、提供する、例えば視聴者から直接、視聴料金を徴収するケーブルテレビ会社等である。

【００６４】

また、システムホルダ（ＳＨ）が、電子マネーの発行機関等、電子マネー決済処理インフラの提供機関である場合、コンテンツクリエイタ（ＣＣ）は、電子マネーによって利用（購入）可能なコンテンツ、商品の提供機関であり、サービスプロバイダ（ＳＰ）は、コンテンツクリエイタ（ＣＣ）から提供されるコンテン

ツ、商品を電子マネーを利用可能なショップとして実現した販売店となる。この場合のユーザデバイスは、電子マネーを入力可能なＩＣカード等になる。

【００６５】

この他にも、様々なタイプのシステムホルダ（ＳＨ）があり、システムホルダに応じてコンテンツクリエイタ（ＣＣ）、サービスプロバイダ（ＳＰ）、ユーザデバイスが構成される。すなわち、システムホルダ（ＳＨ）は、コンテンツクリエイタ（ＣＣ）、サービスプロバイダ（ＳＰ）、ユーザデバイスによって利用可能なコンテンツ、サービスの提供を可能とするためのコンテンツまたはサービスの流通インフラを提供、管理する機関として定義される。

【００６６】

ここでは、前述の登録局（ＲＡ）の機能をシステムホルダ（ＳＨ）が担う構成とすることにより、ユーザにとって利用し易いコンテンツまたはサービスの流通構成について説明する。

【００６７】

まず、図５を用いて、前述の登録局（ＲＡ）の機能をシステムホルダ（ＳＨ）に付与しない形態での公開鍵暗号方式によるコンテンツまたはサービスの流通構成について説明する。

【００６８】

図５に示すように、ユーザが利用可能なサービスは様々、存在するが、各々が独自の公開鍵暗号方式、すなわち独自の審査、独自の登録により特定のサービスにおいてのみ有効な独自の公開鍵証明書を発行して特定サービスの提供を行なっている。この従来型のサービス提供構成を示したのが図５である。図５では、サービスＡを提供するグループ５１０と、サービスＢを提供するグループ５２０を示している。

【００６９】

サービスＡを提供するグループ５１０には、サービスＡの提供のために利用可能な公開鍵証明書発行局（ＩＡ－Ａ）５１１、公開鍵証明書の利用を要求するサービスプロバイダ（ＳＰ）５１４、ユーザ（デバイス）５１５の登録管理を実行する登録局（ＲＡ－Ａ）５１２が設置され、登録局５１２は、例えば公的な審査

機関５１３の審査に基づいて、サービスプロバイダ５１４、ユーザ（デバイス）５１５の登録を行ない、公開鍵証明書発行局（ＩＡ－Ａ）５１１に証明書の発行を要求し、サービスプロバイダ５１４、ユーザ（デバイス）５１５の管理を行なう。なお、公開鍵証明書発行局（ＩＡ－Ａ）５１１と登録局５１２によって認証局Ａ（ＣＡ－Ａ）が構成される。

【００７０】

サービスＢを提供するグループ５２０には、サービスＢの提供のために利用可能な公開鍵証明書発行局（ＩＡ－Ｂ）５２１、公開鍵証明書の利用を要求するサービスプロバイダ（ＳＰ）５２４、ユーザ（デバイス）５２５の登録管理を実行する登録局（ＲＡ－Ｂ）５２２が設置され、登録局５２２は、例えば公的な審査機関５２３の審査に基づいて、サービスプロバイダ５２４、ユーザ（デバイス）５２５の登録を行ない、公開鍵証明書発行局（ＩＡ－Ｂ）５２１に証明書の発行を要求し、サービスプロバイダ５１４、ユーザ（デバイス）５２５の管理を行なう。なお、公開鍵証明書発行局（ＩＡ－Ｂ）５２１と登録局５２２によって認証局Ｂ（ＣＡ－Ｂ）が構成される。

【００７１】

このような構成において、例えばサービスＡの提供を受けるために、登録局（ＲＡ－Ａ）５１２を介して登録を行い、サービスＡで適用可能な公開鍵証明書の発行を受けているユーザ５１５が、サービスＢのサービスを受けようとした場合は、発行済みの公開鍵証明書は使用できない。ユーザ５１５が、サービスＢのサービスを受けるためには、サービスＢを管轄する登録局（ＲＡ－Ｂ）５２２を介して新たな登録手続きを行なって新たな公開鍵証明書の発行を受けることが必須となる。

【００７２】

これを解決するには、図５に示す公開鍵証明書発行局と登録局によって構成される認証局（ＣＡ）相互間で認証する構成としたり、あるいは認証局（ＣＡ）を階層構造とすることが考えられるが、認証局（ＣＡ）の処理負担の増加、認証局（ＣＡ）構造の複雑化を招くという欠点がある。一方、ユーザが複数のサービスを受けるためにサービス毎の複数の公開鍵証明書をデバイス中に格納する構成と

すると、ユーザデバイスの記憶領域を公開鍵証明書の記憶のために多く使用することになる。このような構成は、例えばユーザデバイスがＩＣカードのような限定されたメモリ領域を有するデバイスにおいては問題である。

【００７３】

また、図５のユーザデバイス５１５とユーザデバイス５２５との相互間で、例えばオフラインでの相互認証を行なおうとした場合、それぞれの管轄認証局（ＣＡ）が異なっているため認証処理が実行できないことになる。相互認証を有効に実行するためには、デバイス自身管轄の認証局の公開鍵と、相手デバイスの管轄の認証局の公開鍵の層法をデバイスに格納することが必要となり、様々な相手デバイスとの認証が必要となる場合には、格納公開鍵の数もさらに増加することになる。

【００７４】

このように、サービス毎に独立した管理を行なう図５の構成では、様々な問題が発生する。この問題を解決するのが図６に示すシステムホルダ（ＳＨ）をルート登録局（ルートＲＡ）の下の階層に設定した構成である。

【００７５】

図６の構成について説明する。図６の構成は、先の図５の構成に対応した構成であり、図の左側がサービスＡ、右側がサービスＢを提供するサービスプロバイダ集合が含まれる。サービスプロバイダ６０４は、サービスＡの提供主体であり、サービスプロバイダ６０７は、サービスＢの提供主体である。

【００７６】

サービスプロバイダ６０４、ユーザ（デバイス）６０５、サービスプロバイダ６０７、ユーザ（デバイス）６０８が認証対象者、すなわち公開鍵暗号化方式によるデータ送受信を実行する主体となる。図６では、２つのサービスＡ，Ｂについての構成を示しているが、サービスは一般に多数存在することができる。

【００７７】

システムホルダＡ，６０３は、前述の登録局（ＲＡ）としての役割、機能を実行する。管轄下にある認証対象者のサービスプロバイダ６０４、ユーザ（デバイス）６０５は、システムホルダＡ，６０３に対して、自己の使用する公開鍵に対

応する公開鍵証明書の発行を要求する。システムホルダＢ，６０６は、管轄下にある認証対象者のサービスプロバイダ６０７、ユーザ（デバイス）６０８からの公開鍵証明書の発行要求を受領する。

【００７８】

システムホルダＡ，６０３、システムホルダＢ，６０６は、各サービスにおける対象（サービスに参加するエンティティ、機器）を認証する。また、システムホルダＡ，６０３、システムホルダＢ，６０６は、各サービスにおける対象（サービスに参加するエンティティ、機器、ユーザ）の使用する公開鍵の公開鍵証明書発行要求を受領し、これをルート登録局（ルートＲＡ）６０２を介して、あるいは直接、公開鍵証明書発行局（ＩＡ）６０１に転送する。

【００７９】

ルート登録局（ルートＲＡ）６０２を介する処理の場合、ルート登録局（ルートＲＡ）６０２は、予め実行された認証が成立済みのシステムホルダＡ，６０３、システムホルダＢ，６０６から公開鍵証明書発行要求を受理する。すなわち、ルート登録局（ルートＲＡ）６０２が公開鍵証明書発行要求を受領するのは、ルート登録局（ルートＲＡ）６０２によって認証されたシステムホルダＡ，６０３、システムホルダＢ，６０６からの要求である。なお、システムホルダＡ，６０３、システムホルダＢ，６０６と直接、公開鍵証明書発行局（ＩＡ）６０１とのデータ通信を行なう場合も認証が成立したことが条件とされる。

【００８０】

図６において、サービスプロバイダ６０４、サービスプロバイダ６０７は、例えば音楽データ、画像データ、ゲームプログラム等のコンテンツ配信のサービス提供を実行するサービスプロバイダであり、例えば、先に図４を用いて説明した各種のサービスを提供するサービス提供主体によって構成される。

【００８１】

システムホルダＡ，６０３、システムホルダＢ，６０６は、サービスプロバイダ６０４、サービスプロバイダ６０７の提供するサービスを実現するインフラを管理する機関であり、図４を用いて説明したように、携帯電話通信インフラ提供者、電子マネー・カード発行機関等によって構成される。

【００８２】

本構成の特徴は、コンテンツ提供、サービス提供を実現するインフラを提供または管理する機関であるシステムホルダが公開鍵証明書による認証、データ通信を実行するサービスプロバイダ、ユーザデバイスの公開鍵証明書発行手続き仲介、登録管理を行なう点である。システムホルダは、コンテンツ提供、サービス提供を実現するインフラを提供または管理する機関であるので、そのインフラを利用するユーザ、あるいはサービスプロバイダの管理を行なっている場合が多く、管理用のデータベースを備えている構成であることが多い。このような管理データベースを利用して公開鍵証明書発行先の管理を併せて行なうことで効率的なユーザ、あるいはサービスプロバイダ管理が実行可能となる。

【００８３】

また、例えば新たな通信インフラが構築され、新たなシステムホルダが出現した場合に、その新規システムホルダを既存のルート登録局（ルートＲＡ）、公開鍵証明書発行局（ＩＡ）の管轄下に設定することで、容易に新規のインフラを利用した公開鍵証明書発行構成が実現され、新たなインフラを利用したサービスの提供がいち早く実現できる。

【００８４】

ユーザデバイスは、１つの公開鍵証明書を格納するのみで、様々なサービスを利用可能となる。すなわち、図６の構成では、１つのルート登録局（ルートＲＡ）、公開鍵証明書発行局（ＩＡ）が様々なシステムホルダ、サービスプロバイタに対応して設定されているので、ユーザデバイスは１つの公開鍵証明書を持つことにより、異なるサービスにおいて利用可能となる。また、異なるシステムホルダの管轄下のユーザデバイス相互間においても、１つの共通する公開鍵証明書発行局（ＩＡ）の発行する公開鍵を用いることにより、相互認証が可能となる。

【００８５】

[アクセス制御サーバを構成要素としたデータ配信構成]

次に、上述のシステムホルダを用いた構成において、さらに、アクセス制御サーバを構成要素とした例について説明する。図７にアクセス制御サーバを設けた公開鍵証明書を用いたデータ配信システムの構成ブロック図を示す。

【００８６】

図７の構成について説明する。公開鍵証明書を発行する公開鍵証明書発行局（ＩＡ）７０１、１以上のシステムホルダを管轄するルートＲＡ７０２、１以上のサービスプロバイダ、デバイスを管轄するシステムホルダ７０３，７５０、ユーザデバイスに対してコンテンツの配信等、様々なサービスの提供を実行するサービスプロバイダ７０５，７０６，７０７、サービスプロバイダからのサービス提供を受けるユーザデバイス７０８，７０９を有し、さらに、本構成ではアクセス制御サーバ７１０、アクセス制御サーバ登録サーバ７２０を有する。本構成において、サービスプロバイダ、ユーザデバイスが主たるデータ送受信者、すなわち公開鍵暗号化方式によるデータ送受信を実行する主体となる。

【００８７】

図７の構成では、アクセス制御サーバ７１０は、１つのシステムホルダ７０３に対応して設定されており、システムホルダの７０３管轄するサービスプロバイダ７０５～７０７に対するデバイス７０８，７０９からのアクセスの可否を決定するためのアクセス許可書発行処理を実行する。すなわち、ユーザデバイス７０８，７０９に対してアクセスの認められたサービスプロバイダを設定したアクセス許可書を発行する。ユーザデバイス７０８，７０９は、サービスプロバイダ７０５～７０７に対するアクセス時にアクセス制御サーバ７１０の発行したアクセス許可書をサービスプロバイダ７０５～７０７に提示する。サービスプロバイダは、ユーザデバイス７０８，７０９から受領したアクセス許可書に基づいて、アクセスの認否を判定する。アクセス許可書については後段で詳細に説明する。

【００８８】

また、アクセス制御サーバ登録サーバ７２０は、システムホルダ７０３の管轄するサービスプロバイダ７０５～７０７とのデータ通信を実行し、ユーザデバイス７０８，７０９からのアクセス許可書発行要求をサービスプロバイダ７０５～７０７を介して受信し、受信したユーザデバイス７０８，７０９からのアクセス許可書発行要求に基づいてアクセス制御サーバ７１０にアクセス許可書の発行依頼を行なう。

【００８９】

なお、図７に示す各エンティテイ（ルートＲＡ，ＳＨ，ＳＰ，ユーザデバイス）は公開鍵証明書（ＩＡ）の発行した公開鍵証明書を有し、各エンティテイ間のデータ通信は、公開鍵ベースでの認証処理を実行して、必要に応じてセッション鍵を生成してセッション鍵での暗号化を実行してデータ通信を実行する。

【００９０】

図７の構成は、アクセス制御サーバ７１０、アクセス制御サーバ登録サーバ７２０は、１つのシステムホルダ７０３に対応して設定された構成であるが、アクセス制御サーバ、アクセス制御サーバ登録サーバを複数のシステムホルダ共通に利用可能とする構成としてもよい。

【００９１】

複数のシステムホルダに共通に利用可能なアクセス制御サーバ、アクセス制御サーバ登録サーバを有する構成を図８に示す。図８において、アクセス制御サーバ８１０、アクセス制御サーバ登録サーバ８２０は、複数のシステムホルダ７０３，７５０に共通に利用可能な構成である。システムホルダ７０３管轄下にあるサービスプロバイダ７０５～７０７、ユーザデバイス７０８，７０９、さらにシステムホルダ７５０の管轄下にあるサービスプロバイダ７５１、ユーザデバイス７５２は、すべてアクセス制御サーバ８１０、アクセス制御サーバ登録サーバ８２０によって管理され、アクセス制御サーバ８１０の発行するアクセス許可書を利用する。

【００９２】

[アクセス許可書]

次に、図７、図８に示すアクセス制御サーバの発行するアクセス許可書について説明する。アクセス許可書の発行形態は大きく分けて２種類ある。第１の方式は、１つのサービスプロバイダに対してのみ有効なサービスプロバイダ固有のアクセス許可書（方式Ａ）であり、第２の方式は、複数のサービスプロバイダに対して共通に有効なアクセス許可書（方式Ｂ）である。

【００９３】

これら２つの方式の例を図９に示す。方式Ａは、サービスプロバイダ（ＳＰ）毎に、それぞれサービスプロバイダの要求するデータ項目を含む様式で作成され

、１つのアクセス許可書が１つのサービスプロバイダにのみ有効な方式である。一方、方式Ｂは、複数のサービスプロバイダに共通に利用可能な方式であり、各サービスプロバイダの要求するデータ項目をそれぞれ含む様式で作成される。方式Ａの場合、ユーザデバイスは、アクセスの実行を行なうサービスプロバイダ個々のアクセス許可書を保有することになる。一方、方式Ｂの場合は、１つのアクセス許可書のみを格納するのみで、複数のサービスプロバイダに対して対処可能となる。

【００９４】

図１０に、方式Ｂの場合のアクセス許可書のサンプルを示す。アクセス許可書は、アクセス制御サーバ（ＡＣＳ）が設定する固定フィールドと、各サービスプロバイダ（ＳＰ）が設定するオプションフィールド、さらにアクセス制御サーバ（ＡＣＳ）による署名フィールドに区分される。

【００９５】

固定フィールドには、アクセス許可書のシリアル番号、有効期限、アクセス許可書の発行対象者の公開鍵証明書（ＰＫＣ）のシリアル番号、アクセス許可書のフォーマットのバージョン番号、アクセス許可書発行者（この場合はＡＣＳ）の発行者識別名、さらに、アクセス許可書に付加された署名のアルゴリズム（例えば楕円曲線暗号方式、あるいはＲＳＡ方式等）を識別する署名方式が含まれる。

【００９６】

シリアル番号は、アクセス許可書発行者（この場合はＡＣＳ）によって設定されるアクセス許可書のシリアルナンバである。

有効期限(validity)は、証明書の有効期限である開始日時、終了日時が記録される。

公開鍵証明書（ＰＫＣ）のシリアル番号は、このアクセス許可書を使用するユーザデバイスが保有する公開鍵証明書のシリアル番号が記録される。

バージョン番号は、アクセス許可書のフォーマットのバージョンを示す。

発行者式別名は、アクセス許可書の発行者、すなわちアクセス制御サーバ（ＡＣＳ）の名称が識別可能な形式（Distinguished Name）で記録されるフィールドである。

署名方式は、アクセス許可書に対する署名の署名アルゴリズムとそのパラメータを記録するフィールドである。なお、署名アルゴリズムとしては、楕円曲線暗号およびＲＳＡがあり、楕円曲線暗号が適用されている場合はパラメータおよび鍵長が記録され、ＲＳＡが適用されている場合には鍵長が記録される。

【００９７】

オプションフィールドは、各サービスプロバイダ（ＳＰ）が独自に設定可能なフィールドであり、それぞれのサービスプロバイダの識別名、データサイズ、内容によって構成されるサービスプロバイダ単位のフィールドによって構成される。内容の具体例については図１１で説明する。さらに、オプションフィールドの全体のデータサイズが記録される。

【００９８】

署名フィールドは、アクセス許可書発行者（この場合はＡＣＳ）の署名がなされるフィールドである。

【００９９】

図１０に示すオプションフィールド中の、サービスプロバイダによって設定される「内容」のフィールド構成例を図１１に示す。

【０１００】

図１１の方式イ）は、ユーザ情報を「内容」として格納した例である。例えば、性別、年齢、役職等の様々なユーザ情報を格納する。これらのユーザ情報は多くの場合、プライベートな秘密情報を含み、サービスプロバイダの固有秘密鍵を用いて暗号化されて格納される。この場合、暗号鍵バージョンが併せて記録され、サービスプロバイダは、自己の所有する秘密鍵で、必要に応じてユーザ情報を復号する。

【０１０１】

図１１の方式ロ）は、「内容」としてユーザＩＤのみを格納する構成であり、サービスプロバイダは、ユーザＩＤに基づいて自身で保有するユーザ情報データベースにアクセス可能なリンクを形成して、必要なユーザ情報を取得可能とした構成である。本方式は、ユーザ情報をサービスプロバイダの保有するデータベースで一元管理可能として、重複したデータをアクセス許可書に格納する必要を排

除したものであり、個人情報の漏洩等の問題発生の可能性を押さえたセキュリティの高い構成である。

【０１０２】

図１１の方式ハ）は、「内容」としてユーザに対してアクセスを許可したか否かを示す情報のみを格納する構成であり、サービスプロバイダは、例えばユーザに対してアクセスを許可した場合は「１」、しない場合は「０」を設定する。本構成は、ユーザの個人情報によらず、ユーザ登録を行なったか否かのみに基づいてアクセス許可を設定する構成において特に有効である。また、本構成は、必要なデータ量が極めて少ないのでアクセス許可書のデータ量を削減できる。さらに、複数のサービスプロバイダに対して、ＳＰ１：０，ＳＰ２：１，…ＳＰｎ，０等、一括したアクセス認否用のビットを割り当てる構成とすることにより、さらにデータ量を削減できる。

【０１０３】

[電子署名および認証処理]

次に、本発明のアクセス制御システムにおけるアクセス許可書の発行処理および利用において、各エンティティで実行される電子署名生成処理、検証処理、さらに認証処理の概要を説明する。電子署名および相互認証処理について説明した後に、本発明のアクセス許可書を利用した具体的処理の詳細を説明する。

【０１０４】

(電子署名)

公開鍵暗号方式を用いた電子署名の生成方法を図１２を用いて説明する。図１２に示す処理は、ＥＣ－ＤＳＡ（(Elliptic Curve Digital Signature Algorithm)、IEEE P1363/D3）を用いた電子署名データの生成処理フローである。なお、ここでは公開鍵暗号として楕円曲線暗号（Elliptic Curve Cryptography（以下、ＥＣＣと呼ぶ））を用いた例を説明する。なお、本発明のデータ処理装置においては、楕円曲線暗号以外にも、同様の公開鍵暗号方式における、例えばＲＳＡ暗号（(Rivest、Shamir、Adleman)など（ANSI X9.31））を用いることも可能である。

【０１０５】

図１２の各ステップについて説明する。ステップＳ１において、ｐを標数、ａ、ｂを楕円曲線の係数（楕円曲線：$y^2=x^3+ax+b$）、Ｇを楕円曲線上のベースポイント、ｒをＧの位数、Ｋｓを秘密鍵（０＜Ｋｓ＜ｒ）とする。ステップＳ２おいて、メッセージＭのハッシュ値を計算し、f=Hash(M)とする。

【０１０６】

ここで、ハッシュ関数を用いてハッシュ値を求める方法を説明する。ハッシュ関数とは、メッセージを入力とし、これを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ異なる入力データを探し出すことが困難である特徴を有する。ハッシュ関数としては、ＭＤ４、ＭＤ５、ＳＨＡ－１などが用いられる場合もあるし、ＤＥＳ－ＣＢＣが用いられる場合もある。この場合は、最終出力値となるＭＡＣ（チェック値：ＩＣＶに相当する）がハッシュ値となる。

【０１０７】

続けて、ステップＳ３で、乱数ｕ（０＜ｕ＜ｒ）を生成し、ステップＳ４でベースポイントをｕ倍した座標Ｖ（Ｘｖ，Ｙｖ）を計算する。なお、楕円曲線上の加算、２倍算は次のように定義されている。

【０１０８】

【数１】

P=(Ｘａ，Ｙａ),Q=(Ｘｂ，Ｙｂ),R=(Ｘｃ,Ｙｃ)=P+Qとすると、

P≠Qの時（加算）、

$Xc=\lambda^2-Xa-Xb$

$Yc=\lambda\times(Xa-Xc)-Ya$

$\lambda=(Yb-Ya)/(Xb-Xa)$

P=Qの時（2倍算）、

$Xc=\lambda^2-2Xa$

$Yc=\lambda\times(Xa-Xc)-Ya$

$\lambda=(3(Xa)^2+a)/(2Ya)$

【０１０９】

これらを用いて点Ｇのｕ倍を計算する（速度は遅いが、最もわかりやすい演算方法として次のように行う。Ｇ、２×Ｇ、４×Ｇ・・を計算し、uを2進数展開して1が立っているところに対応する2^{i}×Ｇ（Ｇをｉ回２倍算した値（ｉはｕのＬＳＢから数えた時のビット位置））を加算する。

【０１１０】

ステップＳ５で、ｃ＝Ｘｖｍｏｄ　ｒを計算し、ステップＳ６でこの値が０になるかどうか判定し、０でなければステップＳ７でｄ＝［（ｆ＋ｃＫｓ）／ｕ］ｍｏｄ　ｒを計算し、ステップＳ８でｄが０であるかどうか判定し、ｄが０でなければ、ステップＳ９でｃおよびｄを電子署名データとして出力する。仮に、ｒを１６０ビット長の長さであると仮定すると、電子署名データは３２０ビット長となる。

【０１１１】

ステップＳ６において、ｃが０であった場合、ステップＳ３に戻って新たな乱数を生成し直す。同様に、ステップＳ８でｄが０であった場合も、ステップＳ３に戻って乱数を生成し直す。

【０１１２】

次に、公開鍵暗号方式を用いた電子署名の検証方法を、図１３を用いて説明する。ステップＳ１１で、Ｍをメッセージ、pを標数、a、bを楕円曲線の係数（楕円曲線：$y^{2}=x^{3}+ax+b$）、Ｇを楕円曲線上のベースポイント、ｒをＧの位数、ＧおよびＫｓ×Gを公開鍵（０＜Ｋｓ＜ｒ）とする。ステップＳ１２で電子署名データｃおよびｄが０＜ｃ＜ｒ、０＜ｄ＜ｒを満たすか検証する。これを満たしていた場合、ステップＳ１３で、メッセージＭのハッシュ値を計算し、ｆ＝Ｈａｓｈ（Ｍ）とする。次に、ステップＳ１４でh=1/d mod rを計算し、ステップＳ１５でｈ１＝ｆｈ　ｍｏｄ　ｒ、ｈ２=ｃｈ　ｍｏｄ　ｒを計算する。

【０１１３】

ステップＳ１６において、既に計算したｈ１およびｈ２を用い、点Ｐ＝（Ｘｐ，Ｙｐ）＝ｈ１×Ｇ＋ｈ２・Ｋｓ×Ｇを計算する。電子署名検証者は、公開鍵ＧおよびＫｓ×Ｇを知っているので、図１２のステップＳ４と同様に楕円曲線上の

点のスカラー倍の計算ができる。そして、ステップＳ１７で点Ｐが無限遠点かどうか判定し、無限遠点でなければステップＳ１８に進む（実際には、無限遠点の判定はステップＳ１６でできてしまう。つまり、Ｐ＝（Ｘ，Ｙ）、Ｑ＝（Ｘ，－Ｙ）の加算を行うと、λが計算できず、Ｐ＋Ｑが無限遠点であることが判明している）。ステップＳ１８でＸｐ ｍｏｄ ｒを計算し、電子署名データｃと比較する。最後に、この値が一致していた場合、ステップＳ１９に進み、電子署名が正しいと判定する。

【０１１４】

電子署名が正しいと判定された場合、データは改竄されておらず、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したことがわかる。

【０１１５】

ステップＳ１２において、電子署名データｃまたはｄが、０＜ｃ＜ｒ、０＜ｄ＜ｒを満たさなかった場合、ステップＳ２０に進む。また、ステップＳ１７において、点Ｐが無限遠点であった場合もステップＳ２０に進む。さらにまた、ステップＳ１８において、Ｘｐ ｍｏｄ ｒの値が、電子署名データｃと一致していなかった場合にもステップＳ２０に進む。

【０１１６】

ステップＳ２０において、電子署名が正しくないと判定された場合、データは改竄されているか、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したのではないことがわかる。

【０１１７】

（相互認証処理）

データ送受信を実行する２つの手段間では、相互に相手が正しいデータ通信者であるか否かを確認して、その後に必要なデータ転送を行なうことが行われる。相手が正しいデータ通信者であるか否かの確認処理が相互認証処理である。相互認証処理時にセッション鍵の生成を実行して、生成したセッション鍵を共有鍵として暗号化処理を実行してデータ送信を行なう構成が１つの好ましいデータ転送方式である。

【０１１８】

共通鍵暗号方式を用いた相互認証方法を、図１４を用いて説明する。図１４において、共通鍵暗号方式としてＤＥＳを用いているが、同様な共通鍵暗号方式であればいずれでもよい。

【０１１９】

まず、Ｂが６４ビットの乱数Ｒｂを生成し、Ｒｂおよび自己のＩＤであるＩＤ（ｂ）をＡに送信する。これを受信したＡは、新たに６４ビットの乱数Ｒａを生成し、Ｒａ、Ｒｂ、ＩＤ（ｂ）の順に、ＤＥＳのＣＢＣモードで鍵Ｋａｂを用いてデータを暗号化し、Ｂに返送する。

【０１２０】

これを受信したＢは、受信データを鍵Ｋａｂで復号化する。受信データの復号化方法は、まず、暗号文Ｅ１を鍵Ｋａｂで復号化し、乱数Ｒａを得る。次に、暗号文Ｅ２を鍵Ｋａｂで復号化し、その結果とＥ１を排他的論理和し、Ｒｂを得る。最後に、暗号文Ｅ３を鍵Ｋａｂで復号化し、その結果とＥ２を排他的論理和し、ＩＤ(ｂ)を得る。こうして得られたＲａ、Ｒｂ、ＩＤ(ｂ)の内、ＲｂおよびＩＤ(ｂ)が、Ｂが送信したものと一致するか検証する。この検証に通った場合、ＢはＡを正当なものとして認証する。

【０１２１】

次にＢは、認証後に使用するセッション鍵（Session Key（以下、Ｋｓｅｓとする））を生成する（生成方法は、乱数を用いる）。そして、Ｒｂ、Ｒａ、Ｋｓｅｓの順に、ＤＥＳのＣＢＣモードで鍵Ｋａｂを用いて暗号化し、Ａに返送する。

【０１２２】

これを受信したＡは、受信データを鍵Ｋａｂで復号化する。受信データの復号化方法は、Ｂの復号化処理と同様であるので、ここでは詳細を省略する。こうして得られたＲｂ、Ｒａ、Ｋｓｅｓの内、ＲｂおよびＲａが、Ａが送信したものと一致するか検証する。この検証に通った場合、ＡはＢを正当なものとして認証する。互いに相手を認証した後には、セッション鍵Ｋｓｅｓは、認証後の秘密通信のための共通鍵として利用される。

【０１２３】

なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【０１２４】

次に、公開鍵暗号方式である１６０ビット長の楕円曲線暗号を用いた相互認証方法を、図１５を用いて説明する。図１５において、公開鍵暗号方式としてＥＣＣを用いているが、前述のように同様な公開鍵暗号方式であればいずれでもよい。また、鍵サイズも１６０ビットでなくてもよい。図１５において、まずＢが、６４ビットの乱数Ｒｂを生成し、Aに送信する。これを受信したＡは、新たに６４ビットの乱数Ｒａおよび標数ｐより小さい乱数Ａｋを生成する。そして、ベースポイントＧをＡｋ倍した点Ａｖ＝Ａｋ×Ｇを求め、Ｒａ、Ｒｂ、Ａｖ（X座標とY座標）に対する電子署名Ａ．Ｓｉｇを生成し、Ａの公開鍵証明書とともにＢに返送する。ここで、ＲａおよびＲｂはそれぞれ６４ビット、ＡｖのＸ座標とＹ座標がそれぞれ１６０ビットであるので、合計４４８ビットに対する電子署名を生成する。電子署名の生成方法は図１２で説明したので、その詳細は省略する。

【０１２５】

公開鍵証明書を利用する際には、利用者は自己が保持する公開鍵証明書発行局（ＩＡ）の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の公開鍵証明書発行局（ＩＡ）の公開鍵を保持している必要がある。なお、電子署名の検証方法については、図１３で説明したのでその詳細は省略する。

【０１２６】

図１５に戻って説明を続ける。Ａの公開鍵証明書、Ｒａ、Ｒｂ、Ａｖ、電子署名Ａ．Ｓｉｇを受信したＢは、Ａが送信してきたＲｂが、Ｂが生成したものと一致するか検証する。その結果、一致していた場合には、Ａの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Ａの公開鍵を取り出す。そして、取り出したＡの公開鍵を用い電子署名Ａ．Ｓｉｇを検証する。電子署名の検証方法は図１３で説明したので、その詳細は省略する。電子署名の検証に成功した後、ＢはＡを正当なものとして認証する。

【０１２７】

次に、Ｂは、標数ｐより小さい乱数Ｂｋを生成する。そして、ベースポイントＧをＢｋ倍した点Ｂｖ＝Ｂｋ×Ｇを求め、Ｒｂ、Ｒａ、Ｂｖ（Ｘ座標とＹ座標）に対する電子署名Ｂ．Ｓｉｇを生成し、Ｂの公開鍵証明書とともにＡに返送する。

【０１２８】

Ｂの公開鍵証明書、Ｒｂ、Ｒａ、Ａｖ、電子署名Ｂ．Ｓｉｇを受信したＡは、Ｂが送信してきたＲａが、Ａが生成したものと一致するか検証する。その結果、一致していた場合には、Ｂの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Ｂの公開鍵を取り出す。そして、取り出したＢの公開鍵を用い電子署名Ｂ．Ｓｉｇを検証する。電子署名の検証に成功した後、ＡはＢを正当なものとして認証する。

【０１２９】

両者が認証に成功した場合には、ＢはＢｋ×Ａｖ（Ｂｋは乱数だが、Ａｖは楕円曲線上の点であるため、楕円曲線上の点のスカラー倍計算が必要）を計算し、ＡはＡｋ×Ｂｖを計算し、これら点のＸ座標の下位６４ビットをセッション鍵として以降の通信に使用する（共通鍵暗号を６４ビット鍵長の共通鍵暗号とした場合）。もちろん、Ｙ座標からセッション鍵を生成してもよいし、下位６４ビットでなくてもよい。なお、相互認証後の秘密通信においては、送信データはセッション鍵で暗号化されるだけでなく、電子署名も付されることがある。

【０１３０】

電子署名の検証や受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【０１３１】

このような相互認証処理において、生成したセッション鍵を用いて、送信データを暗号化して、相互にデータ通信を実行する。

【０１３２】

[アクセス許可書の発行および利用]

(使用する用語の説明)

次に、アクセス許可書の発行処理および利用における処理について、順次説明する。なお、以下の説明において使用される用語についての説明を図１６に示す。これらについて簡単に説明する。鍵をＫとして表記し、サフィックスとして公開鍵はＰ、秘密鍵はＳを付加し、さらに所有者識別子（例えばａ）を付加する。相互認証の際に生成され、暗号化、復号化処理に適用されるセッション鍵をＫｓとする。Ａが発行したＢの公開鍵証明書をＡ≪Ｂ≫とする。データの暗号化は、例えばセッション鍵Ｋｓでデータ（ｄａｔａ）を暗号化した場合は、E_{Ks}（ｄａｔａ）として示す。同様の復号は、D_{Ks}（ｄａｔａ）として示す。署名処理は、例えばデータ（ｄａｔａ）をＡの秘密鍵Ｋｓａで署名した場合は、｛ｄａｔａ｝Ｓｉｇ・Ｋｓａとして示す。また、署名付き暗号化データは、例えばデータ（ｄａｔａ）をＡの秘密鍵Ｋｓａで署名して生成される（ｄａｔａ‖署名）をセッション鍵Ｋｓで暗号化した場合は、E_{Ks}（｛ｄａｔａ｝Ｓｉｇ・Ｋｓａ）で示す。

【０１３３】

（デバイスに対する１枚目のアクセス許可書の発行処理）

次に、本発明のアクセス制御システムにおいて、ユーザデバイスが、サービスプロバイダのアクセス許可を取得するための処理として、最初のアクセス許可書を取得する処理シーケンスについて説明する。

【０１３４】

この場合の処理順序を、各エンティテイ間でのデータの送受信順序に従って示した図を図１７に示す。図１７に示す番号（ｎ）に従って、最初のアクセス許可書を取得するための処理が進行する。以下、各処理について説明する。

【０１３５】

まず、（１）の処理は、デバイス１７０５がサービスプロバイダ（ＳＰ１１）１７０３のサービスを受けるための許可書を取得するため、サービスプロバイダ（ＳＰ１１）１７０３求めるデータ、例えばユーザデバイスＩＤと、年齢等の各種のユーザ情報、デバイス情報を生成してサービスプロバイダに送信する。なお、データ送信前に、デバイス１７０５とサービスプロバイダ（ＳＰ１１）１７０３間においては相互認証が実行され、セッション鍵E_{Ks1}が生成されている。（１）の処理における送信データは、ユーザデバイスＩＤ（ＵＤＩＤ）と、その他

サービスプロバイダ１７０３の求める情報（ｄａｔａ）を含み、これらにユーザデバイス１７０５の秘密鍵K_{SUD}による署名が実行され、さらに、セッション鍵E_{Ks1}を用いて暗号化処理が実行されたデータ：E_{Ks1}（{ＵＤＩＤ，ｄａｔａ}Ｓｉｇ・K_{SUD}）となる。

【０１３６】

サービスプロバイダ（ＳＰ１１）１７０３は、ユーザデバイス１７０５から受信した暗号化データをセッション鍵E_{Ks1}で復号して、さらに署名検証を行ない、データ内容を審査して、サービスプロバイダ（ＳＰ１１）１７０３の求める審査基準を満たすものである場合は、（２）の処理、すなわち、アクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２に対してアクセス許可書の発行依頼を行なう。

【０１３７】

この（２）の処理において、サービスプロバイダ（ＳＰ１１）１７０３は、前述の図１０を用いて説明したアクセス許可書におけるオプションフィールドの記載事項をアクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２に対して送信する。この場合、図１２の各態様のいずれかに従った「内容」データを含むものとなる。例えば図１２の方式イ）の場合は、サービスプロバイダ１７０３は、ユーザ情報を生成して必要に応じてサービスプロバイダ１７０３の鍵を用いて暗号化して送信データを生成する。図１２の方式ロ）の場合はユーザＩＤのみ、図１２の方式ハ）の場合はアクセス許可書の発行要求を行なうのみでよい。サービスプロバイダ（ＳＰ１１）１７０３の生成したデータを（ｄａｔａ２）とし、サービスプロバイダ（ＳＰ１１）１７０３とアクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２間における相互認証処理の際に生成したセッション鍵E_{Ks2}とすると、（２）の処理で送信されるデータは、E_{Ks2}（{ＳＰＩＤ，ｄａｔａ２}Ｓｉｇ・K_{SSP}）となる。

【０１３８】

アクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２が上記データをサービスプロバイダ（ＳＰ１１）１７０３から受信すると、受信データに基づいてアクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２は、アクセス制御サーバ（Ａ

ＣＳ１）１７０１にアクセス許可書の発行要求を行なう（（３）の処理）。

【０１３９】

次に、アクセス制御サーバ（ＡＣＳ１）１７０１は、要求データに基づいてアクセス許可書（ＡＣＰＭＳ）を生成し、アクセス制御サーバ（ＡＣＳ１）１７０１の署名を実行したデータ：｛ＡＣＰＭＳ｝Ｓｉｇ・K_{SACS1}をアクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２に送信する（（４）の処理）。なお、アクセス制御サーバ（ＡＣＳ１）１７０１とアクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２とのデータ通信は、専用線のように外部からの割込みが排除されるセキュアな通信構成とした場合は、特に暗号化しないデータとして送受信する構成としてよい。通信ラインのセキュリティが不確実である場合は、上記の他のエンティテイ間の通信と同様セッション鍵による暗号化処理を実行してデータ送受信を実行する。

【０１４０】

次に、アクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２は、アクセス制御サーバ（ＡＣＳ１）１７０１からの受信データの署名検証処理を実行して、自分の署名を付加し、さらにセッション鍵で暗号化したデータ：E_{Ks5}（｛｛ＡＣＰＭＳ｝Ｓｉｇ・K_{SACS1}｝K_{SRACS1}）をサービスプロバイダ（ＳＰ１１）１７０３に送信する（（５）の処理）。

【０１４１】

次に、サービスプロバイダ（ＳＰ１１）１７０３は、アクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２からの受信データの署名検証処理を実行して、自分の署名を付加し、さらにセッション鍵で暗号化したデータ：E_{Ks6}（｛｛｛ＡＣＰＭＳ｝Ｓｉｇ・K_{SACS1}｝K_{SRACS1}｝K_{SSP}）をユーザデバイス１７０５に送信する（（６）の処理）。

【０１４２】

ユーザデバイス１７０５は、セッション鍵E_{Ks4}での復号処理の後、署名検証を実行し、アクセス許可書（ＡＣＰＭＳ）を自身のセキュアモジュールに格納する（（７）の処理）。なお、格納の際には、自身の保存鍵K_{str}を用いて暗号化処理を行なって保存することが望ましい。

【０１４３】

（デバイスにすでにアクセス許可書がある場合の新たなアクセス許可書の発行処理）

次に、すでにユーザデバイスがあるサービスプロバイダのアクセス許可書を有しており、新たに他のサービスプロバイダのアクセス許可書を取得する場合の処理について図１８を用いて説明する。

【０１４４】

図１８に示すユーザデバイス１７０５は、すでにサービスプロバイダ（ＳＰ１１）１７０３のアクセス許可書を有しており、新たにサービスプロバイダ（ＳＰ１２）１７０４のアクセス許可書を取得する。まず、ユーザデバイス１７０５は、サービスプロバイダ（ＳＰ１２）１７０４求めるデータ、例えばユーザデバイスＩＤと、年齢等の各種のユーザ情報、デバイス情報を生成してサービスプロバイダ（ＳＰ１２）１７０４に送信する（（８）の処理）。この際の送信データは、先の図１７を用いた説明と同様、ユーザデバイスＩＤ（ＵＤＩＤ）と、その他サービスプロバイダ１７０４の求める情報（ｄａｔａ）を含み、これらにユーザデバイス１７０５の秘密鍵K_{SUD}による署名が実行され、さらに、セッション鍵E_{Ks8}を用いて暗号化処理が実行されたデータ：E_{Ks8}（{ＵＤＩＤ，ｄａｔａ}Ｓｉｇ・K_{SUD}）となる。

【０１４５】

サービスプロバイダ（ＳＰ１２）１７０４は、ユーザデバイス１７０５から受信した暗号化データをセッション鍵E_{Ks}で復号して、さらに署名検証を行ない、データ内容を審査して、サービスプロバイダ（ＳＰ１２）１７０４の求める審査基準を満たすものである場合は、（９）の処理、すなわち、アクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２に対してアクセス許可書の発行依頼を行なう。

【０１４６】

この（９）の処理において、送信されるデータは、前述の図１７の（２）の処理と同様であり、E_{Ks9}（{ＳＰＩＤ，ｄａｔａ２}Ｓｉｇ・K_{SSP}）となる。アクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２が上記データをサービスプ

ロバイダ（ＳＰ１２）１７０４から受信すると、受信データに基づいてアクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２は、アクセス制御サーバ（ＡＣＳ１）１７０１にアクセス許可書の発行要求を行なう（（１０）の処理）。

【０１４７】

次に、アクセス制御サーバ（ＡＣＳ１）１７０１は、要求データに基づいてアクセス許可書（ＡＣＰＭＳ）を生成し、アクセス制御サーバ（ＡＣＳ１）１７０１の署名を実行したデータ：｛ＡＣＰＭＳ｝Ｓｉｇ・K_{SACS1}をアクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２に送信する（（１１）の処理）。なお、アクセス制御サーバ（ＡＣＳ１）１７０１の生成するアクセス許可書は、先に図９，１０を用いて説明したように、複数の方式があり、例えば図９の方式Ａに従う場合は、各サービスプロバイダ毎のアクセス許可書となり、この場合は、サービスプロバイダ（ＳＰ１２）１７０４にのみ有効な新たなアクセス許可書を発行する。図９の方式Ｂに従う場合は、すでにユーザデバイス１７０５の有する既存のアクセス許可書に新たなサービスプロバイダ（ＳＰ１２）１７０４のオプションフィールド（図１０，１１参照）を付加して既存のアクセス許可書の変更処理を実行する。

【０１４８】

次に、アクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２は、アクセス制御サーバ（ＡＣＳ１）１７０１からの受信データの署名検証処理を実行して、自分の署名を付加し、さらにセッション鍵で暗号化したデータ：E_{Ks12}（｛｛ＡＣＰＭＳ｝Ｓｉｇ・K_{SACS1}｝K_{SRACS1}）をサービスプロバイダ（ＳＰ１２）１７０４に送信する（（１２）の処理）。

【０１４９】

次に、サービスプロバイダ（ＳＰ１２）１７０４は、アクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２からの受信データの署名検証処理を実行して、自分の署名を付加し、さらにセッション鍵で暗号化したデータ：E_{Ks13}（｛｛｛ＡＣＰＭＳ｝Ｓｉｇ・K_{SACS1}｝K_{SRACS1}｝K_{SSP}）をユーザデバイス１７０５に送信する（（１３）の処理）。

【０１５０】

ユーザデバイス１７０５は、セッション鍵E_{Ks13}での復号処理の後、署名検証を実行し、アクセス許可書（ＡＣＰＭＳ）を自身のセキュアモジュールに格納する。なお、格納の際には、自身の保存鍵K_{str}を用いて暗号化処理を行なって保存することが望ましい。この場合のアクセス許可書は、方式Ａの形式の場合は、図１８の上段に示すように各サービスプロバイダ毎のアクセス許可書となり、方式Ｂの場合は、図１８の下段に示すように複数のサービスプロバイダに共通のアクセス許可書となる。

【０１５１】

（アクセス許可書の利用）

次に、ユーザデバイスがアクセス許可書を利用してサービスプロバイダからサービス提供を受ける処理について説明する。

【０１５２】

ユーザデバイスは、サービス提供を受けようとするサービスプロバイダとの間で、まず相互認証処理を実行する。相互認証処理が成立し、セッション鍵E_{Ks}が生成されると、ユーザデバイスは、アクセス許可書（ＡＣＰＭＳ）に自身の秘密鍵で署名を行ない、かつセッション鍵で暗号化したデータ：E_{Ks}（｛ＵＤＩＤ，ＡＣＰＭＳ｝Ｓｉｇ・K_{SUD}）をサービスプロバイダに送信する。

【０１５３】

サービスプロバイダは、受信データをセッション鍵E_{Ks}で復号し、さらに署名検証処理を行ない、アクセス許可書（ＡＣＰＭＳ）のチェックを実行して、有効なアクセス許可書であることの確認を行ない、確認されたことを条件としてアクセスを許可する。

【０１５４】

このように、本発明のアクセス制御システムによれば、例えば複数のサービスプロバイダに共通に利用されるアクセス制御サーバが設置され、アクセス制御サーバが規定するフォーマット、手順に従ってアクセス制御が実行されることになるので、各サービスプロバイダは、独自のアクセス制御手順を構築する必要がない。また、各ユーザデバイスにおいても個々のサービスプロバイダに応じたアクセス処理シーケンスを実行することなく、一定シーケンスに従った処理が可能と

なるので、サービスプロバイダ毎のフォーマットデータ、アクセスプログラム等を個別に格納管理する必要がなくなる。

【０１５５】

（アクセス許可書の利用停止処理）

次に、ユーザデバイスがアクセス許可書を利用したサービスプロバイダからのサービス停止を行なう場合の処理について図１９を用いて説明する。

【０１５６】

まず、（２１）の処理は、デバイス１７０５がサービスプロバイダ（ＳＰ１１）１７０３のサービス停止処理を実行するため、サービスプロバイダ（ＳＰ１１）１７０３求めるデータを生成してサービスプロバイダに送信する。なお、送信データは、ユーザデバイスＩＤ（ＵＤＩＤ）と、その他サービスプロバイダ１７０３の求める情報（ｄａｔａ）を含み、これらにユーザデバイス１７０５の秘密鍵K_{SUD}による署名が実行され、さらに、セッション鍵E_{Ks21}を用いて暗号化処理が実行されたデータ：E_{Ks21}（｛ＵＤＩＤ，ｄａｔａ｝Ｓｉｇ・K_{SUD}）となる。

【０１５７】

サービスプロバイダ（ＳＰ１１）１７０３は、ユーザデバイス１７０５から受信した暗号化データをセッション鍵E_{Ks21}で復号して、さらに署名検証を行ない、データ内容を審査して、（２２）の処理、すなわち、アクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２に対してアクセス許可書の削除または変更依頼を行なう。この削除または変更処理態様は、アクセス許可書が前述の図９で説明した方式Ａのサービスプロバイダ毎のアクセス許可書である場合は、許可書削除処理として実行可能であり、方式Ｂの場合は、アクセス許可書変更処理として実行可能である。ただし、削除の場合も例えば一定期間のアクセス停止、あるいは限定された利用のみ可能とする当、様々なアクセス不許可態様があり、許可書自体を削除することなく、許可書にアクセス制限を示す識別子を付加する処理も可能であるので、以下ではアクセス許可書の削除についても変更処理の一態様であるとして説明する。

【０１５８】

アクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２が上記データをサービスプロバイダ（ＳＰ１１）１７０３から受信すると、受信データに基づいてアクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２は、アクセス制御サーバ（ＡＣＳ１）１７０１にアクセス許可書の変更処理要求を行なう（（２３）の処理）。

【０１５９】

次に、アクセス制御サーバ（ＡＣＳ１）１７０１は、要求データに基づいてアクセス許可書（ＡＣＰＭＳ）の変更処理を実行し、変更したアクセス許可書にアクセス制御サーバ（ＡＣＳ１）１７０１の署名を実行したデータを生成して、アクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２に送信する（（２４）の処理）。

【０１６０】

次に、アクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２は、アクセス制御サーバ（ＡＣＳ１）１７０１からの受信データの署名検証処理を実行して、自分の署名を付加し、さらにセッション鍵で暗号化した変更アクセス許可書をサービスプロバイダ（ＳＰ１１）１７０３に送信する（（２５）の処理）。

【０１６１】

次に、サービスプロバイダ（ＳＰ１１）１７０３は、アクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２からの受信データの署名検証処理を実行して、自分の署名を付加し、さらにセッション鍵で暗号化した変更アクセス許可書をユーザデバイス１７０５に送信する（（２６）の処理）。

【０１６２】

ユーザデバイス１７０５は、セッション鍵での復号処理の後、署名検証を実行し、変更アクセス許可書の確認を行ない、変更アクセス許可書に有効なデータがある場合は、自身のセキュアモジュールに格納する（（２７）の処理）。

【０１６３】

（アクセス許可書の失効処理）

上述した処理は、ユーザデバイスが自らアクセス許可書の利用を停止する処理であるが、次に、サービスプロバイダ側から特定ユーザのアクセス許可書の利用

を停止、すなわち失効させる処理について図２０を用いて説明する。

【０１６４】

まず、サービスプロバイダ１７０３は、不正ユーザの検出、あるいはユーザデバイスのアクセス条件が条件を満たさなくなったことが明らかになった場合等、そのユーザのアクセス許可書の失効処理の実行を決定する（（３１）の処理）。

【０１６５】

サービスプロバイダ（ＳＰ１１）１７０３は、アクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２に対してアクセス許可書の変更依頼を行なう（（３２）の処理）。アクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２が上記データをサービスプロバイダ（ＳＰ１１）１７０３から受信すると、受信データに基づいてアクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２は、アクセス制御サーバ（ＡＣＳ１）１７０１にアクセス許可書の変更処理要求を行なう（（３３）の処理）。

【０１６６】

次に、アクセス制御サーバ（ＡＣＳ１）１７０１は、要求データに基づいてアクセス許可書（ＡＣＰＭＳ）の変更処理を実行し、変更したアクセス許可書にアクセス制御サーバ（ＡＣＳ１）１７０１の署名を実行したデータを生成して、アクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２に送信する（（３４）の処理）。

【０１６７】

次に、アクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２は、アクセス制御サーバ（ＡＣＳ１）１７０１からの受信データの署名検証処理を実行して、自分の署名を付加し、さらにセッション鍵で暗号化した変更アクセス許可書をサービスプロバイダ（ＳＰ１１）１７０３に送信する（（３５）の処理）。

【０１６８】

このような処理の後、ユーザデバイス１７０５からのアクセス要求があった場合（（３６）の処理）は、サービスプロバイダ（ＳＰ１１）１７０３は、変更アクセス許可書をユーザデバイス１７０５に送信する（（３７）の処理）。ユーザデバイス１７０５は、変更アクセス許可書の確認を行ない、有効データを含む変

更アクセス許可書がある場合は、自身のセキュアモジュールに格納する（（３８）の処理）。

【０１６９】

（システムホルダによるアクセス許可書の失効処理）

上述した処理は、サービスプロバイダ側から特定ユーザのアクセス許可書の利用を停止、すなわち失効させる処理であったが、次にシステムホルダによるアクセス許可書の失効処理について図２１を用いて説明する。

【０１７０】

まず、システムホルダ２１０１は、不正ユーザの検出、あるいはユーザデバイスのアクセス条件が条件を満たさなくなったことが明らかになった場合等、そのユーザのアクセス許可書の失効処理の実行を決定する（（４１）の処理）。

【０１７１】

システムホルダ２１０１は、アクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２に対してアクセス許可書の変更依頼を行なう（（４２）の処理）。アクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２が上記データをシステムホルダ２１０１から受信すると、受信データに基づいてアクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２は、アクセス制御サーバ（ＡＣＳ１）１７０１にアクセス許可書の変更処理要求を行なう（（４３）の処理）。

【０１７２】

次に、アクセス制御サーバ（ＡＣＳ１）１７０１は、要求データに基づいてアクセス許可書（ＡＣＰＭＳ）の変更処理を実行し、変更したアクセス許可書にアクセス制御サーバ（ＡＣＳ１）１７０１の署名を実行したデータを生成して、アクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２に送信する（（４４）の処理）。

【０１７３】

次に、アクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２は、アクセス制御サーバ（ＡＣＳ１）１７０１からの受信データの署名検証処理を実行して、自分の署名を付加し、さらにセッション鍵で暗号化した変更アクセス許可書を、管轄下のサービスプロバイダ（ＳＰ１１）１７０３、サービスプロバイダ（ＳＰ１

２）１７０４に送信する（（４５）の処理）。

【０１７４】

このような処理の後、ユーザデバイス１７０５からのアクセス要求があった場合（（４６）の処理）は、サービスプロバイダ（ＳＰ１１）１７０３は、変更アクセス許可書をユーザデバイス１７０５に送信する（（４７）の処理）。ユーザデバイス１７０５は、変更アクセス許可書の確認を行ない、有効データを含む変更アクセス許可書がある場合は、自身のセキュアモジュールに格納する（（４８）の処理）。

【０１７５】

[その他のエンティティ間でのアクセス許可書の利用態様]

なお、上述の例ではサービスプロバイダとユーザデバイス間でのアクセス制御について説明したが、システムホルダとサービスプロバイダ間のように異なるエンティテイ間でのアクセス制御にも同様に適用可能である。また、ユーザデバイス相互間でのアクセス制御にも同様に適用できる。例えば一定のフォーマットに従ったアクセス許可書をデバイス相互間でのアクセス時に送受信する構成とすることにより、各ユーザデバイスは、一定のフォーマットに従った送信相手の情報を入手して、アクセス許可書に従ってアクセスの可否を決定することが可能となる。この場合のアクセス許可書は、図１０で説明したアクセス許可書のオプションフィールドにユーザデバイスが独自に設定するフィールドを設ける構成とする。

【０１７６】

デバイス間でのアクセス許可書の利用態様について、図２２を用いて説明する。図２２において、サービスを提供するデバイス（サービス提供デバイス）をデバイス２２０１とし、サービスを受信するデバイス（サービス受信デバイス）をデバイス２２０２とする。

【０１７７】

まず、サービス提供デバイスであるデバイス２２０１は、システムホルダ２１０１に対して、オフラインで自分がサービス提供をしてもよいデバイス情報を含んだアクセス許可書の発行を依頼する。デバイス２２０１は、図１０で説明した

と同様のデバイス間での流通用のアクセス許可書のオプションフィールドに、オフラインで自分がサービス提供をしてもよいデバイス情報を格納したアクセス許可書の発行を依頼する（（５１）の処理）。

【０１７８】

また、サービス受信デバイスであるデバイス２２０２は、システムホルダ２１０１に対して、オフラインで自分がデバイス間において受けられるサービスのアクセス許可書の発行を依頼する（（５２）の処理）。

【０１７９】

システムホルダ２１０１は、アクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２に対してアクセス許可書の発行依頼を行なう（（５３）の処理）。アクセス制御サーバ登録サーバ（ＲＡＣＳ１）は、アクセス制御サーバ（ＡＣＳ１）１７０１にアクセス許可書の発行要求を行なう（（５４）の処理）。

【０１８０】

次に、アクセス制御サーバ（ＡＣＳ１）１７０１は、要求データに基づいてアクセス許可書を生成し、アクセス制御サーバ（ＡＣＳ１）１７０１の署名を実行したデータをアクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２に送信する（（５５）の処理）。次に、アクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２は、アクセス制御サーバ（ＡＣＳ１）１７０１からの受信データの署名検証処理を実行して、自分の署名を付加し、さらにセッション鍵で暗号化したデータをシステムホルダ２１０１に送信する（（５６）の処理）。

【０１８１】

次に、システムホルダ２１０１は、アクセス制御サーバ登録サーバ（ＲＡＣＳ１）１７０２からの受信データの署名検証処理を実行して、自分の署名を付加し、さらにセッション鍵で暗号化したデータをデバイス２２０２に送信する（（５７）の処理）。

【０１８２】

デバイス２２０２は、セッション鍵での復号処理の後、署名検証を実行し、アクセス許可書を自身のセキュアモジュールに格納する（（５８）の処理）。

【０１８３】

アクセス許可書を受領したデバイス２２０２は、デバイス２２０１に対してアクセスする場合、アクセス許可書を提示する。デバイス２２０１は提示されたアクセス許可書に基づいて、即座にアクセス許可、あるいは不許可を判定することが可能となる。

【０１８４】

このデバイス間で有効なアクセス許可書についてもサービス停止処理、失効処理は、前述のサービスプロバイダのアクセス許可書の処理と同様に行なわれる。ただし、更新されたアクセス許可書の配布処理は、システムホルダからデバイスに対する配布処理となる。デバイスがシステムホルダに対して接続するタイミングは、例えば公開鍵証明書の更新処理時等であり、この際に更新されたアクセス許可書を配布することが可能である。

【０１８５】

ただし、サービス提供デバイスがアクセス許可書が更新されたことをサービス受信デバイスに通知して、その通知以降のデバイス間のサービスのやりとりは、サービス受信デバイスがシステムホルダに対して接続がなされたことを条件とする構成とすることで、無効なアクセス許可書の使用を排除することが可能となる。

【０１８６】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０１８７】

【発明の効果】

上述したように、本発明のアクセス制御システムによれば、複数のサービスプロバイダ、デバイスに共通に利用されるアクセス制御サーバが設置され、アクセス制御サーバが規定するフォーマット、手順に従ってアクセス制御が実行されることになるので、各サービスプロバイダ、デバイスは、独自のアクセス制御手順

を構築する必要がなく、容易にアクセス制御を実行することが可能となる。また、サービスを受けるユーザデバイスにおいても個々のサービスプロバイダに応じたアクセス処理シーケンスを実行することなく、一定シーケンスに従った処理が可能となるので、サービスプロバイダ毎のフォーマットデータ、アクセスプログラム等を個別に格納管理する必要がなくなる。

【図面の簡単な説明】

【図１】

公開鍵証明書の例を示す図である。

【図２】

本発明の公開鍵暗号を使用したデータ通信システムの概要を説明する図である。

【図３】

公開鍵暗号を使用したデータ通信システムにおけるシステムホルダと他機関との関係について説明する図である。

【図４】

公開鍵暗号を使用したデータ通信システムにおけるシステムホルダと他機関の具体例を説明する図である。

【図５】

システムホルダをルート登録局に対する階層構造としない場合の公開鍵証明書利用例を説明する図である。

【図６】

システムホルダをルート登録局に対する階層構造とした場合の公開鍵証明書利用例を説明する図である。

【図７】

アクセス制御サーバを構成要素としたシステムの概要（例１）を説明する図である。

【図８】

アクセス制御サーバを構成要素としたシステムの概要（例２）を説明する図である。

【図９】

アクセス許可書の方式例を説明する図である。

【図１０】

アクセス許可書のフォーマットについて説明する図である。

【図１１】

アクセス許可書に含まれる内容について説明する図である。

【図１２】

本発明のシステムにおいて適用可能な署名生成処理について説明する図である。

【図１３】

本発明のシステムにおいて適用可能な署名検証処理について説明する図である。

【図１４】

本発明のシステムにおいて適用可能な相互認証処理について説明する図である。

【図１５】

本発明のシステムにおいて適用可能な相互認証処理について説明する図である。

【図１６】

本発明のシステムの処理において使用される用語を説明する図である。

【図１７】

本発明のアクセス制御システムにおける最初のアクセス許可書発行処理シーケンスを説明する図である。

【図１８】

本発明のアクセス制御システムにおけるアクセス許可書発行処理シーケンスを説明する図である。

【図１９】

本発明のアクセス制御システムにおけるアクセス許可書のサービス停止処理シーケンスを説明する図である。

【図２０】

本発明のアクセス制御システムにおけるアクセス許可書のサービス失効処理シーケンスを説明する図である。

【図２１】

本発明のアクセス制御システムにおけるアクセス許可書のシステムホルダが主体となるサービス失効処理シーケンスを説明する図である。

【図２２】

本発明のアクセス制御システムにおけるデバイス間のアクセス許可書の利用シーケンスを説明する図である。

【符号の説明】

２０１　公開鍵証明書発行局（ＩＡ）

２０２　ルート登録局（ルートＲＡ）

２０３，２０４　登録局（サービスプロバイダＲＡ）

２０５　登録局（ペイメントＲＡ）

２０６　ショップ

２０７　端末

２０８　ユーザデバイス

２０９　ユーザの決済機関

３０１　システムホルダ（ＳＨ）

３０２　コンテンツクリエイタ（ＣＣ）

３０３　サービスプロバイダ（ＳＰ）

３０４　ユーザ（デバイス）

５１１，５２１　公開鍵証明書発行局（ＩＡ）

５１２，５２２　ルート登録局（ルートＲＡ）

５１３，５２３　審査機関

５１４，５２４　サービスプロバイダ

５１５，５２５　ユーザ（デバイス）

６０１　公開鍵証明書発行局（ＩＡ）

６０２　ルート登録局（ルートＲＡ）

６０３，６０６　システムホルダ

６０４，６０７　サービスプロバイダ

６０５，６０８　ユーザ（デバイス）

７０１　公開鍵証明書発行局（ＩＡ）

７０２　ルートＲＡ

７０３，７５０　システムホルダ

７０５，７０６，７０７　サービスプロバイダ

７０８，７０９　ユーザデバイス

７１０　アクセス制御サーバ

７２０　アクセス制御サーバ登録サーバ

７５２　ユーザデバイス

８１０　アクセス制御サーバ

８２０　アクセス制御サーバ登録サーバ

１７０１　アクセス制御サーバ

１７０２　アクセス制御サーバ登録サーバ

１７０３，１７０４　サービスプロバイダ

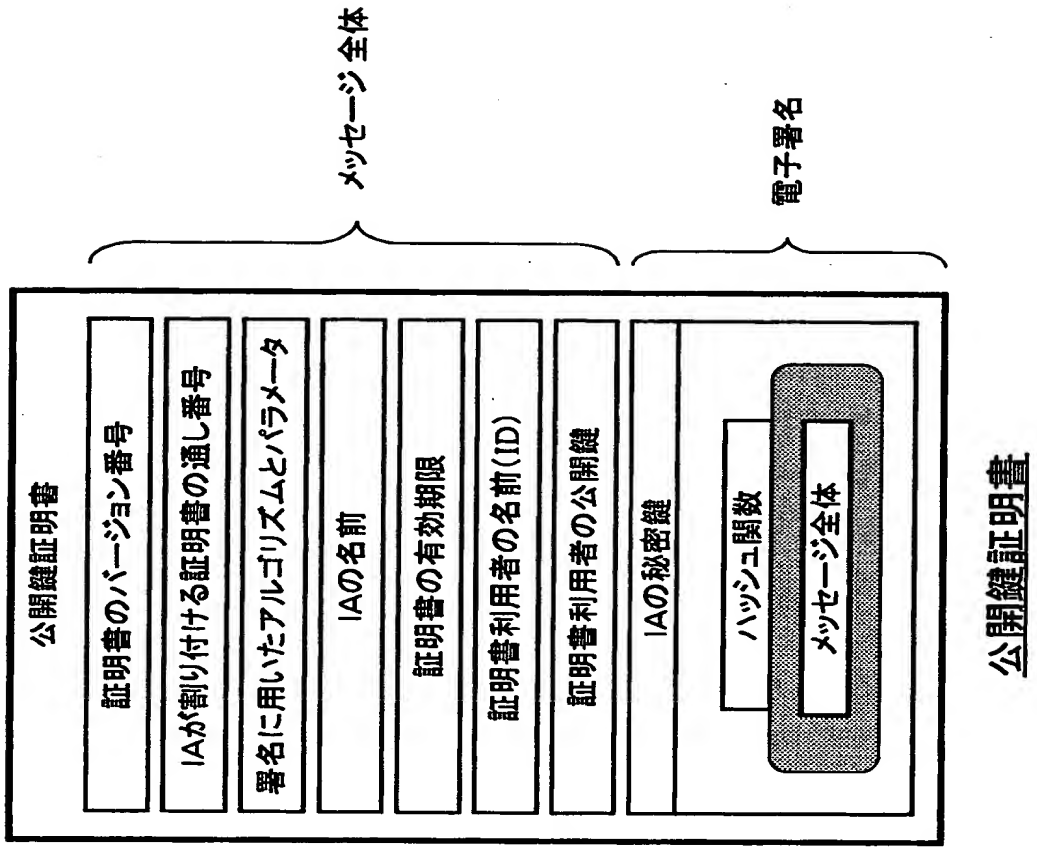
１７０５　ユーザデバイス

２１０１　システムホルダ

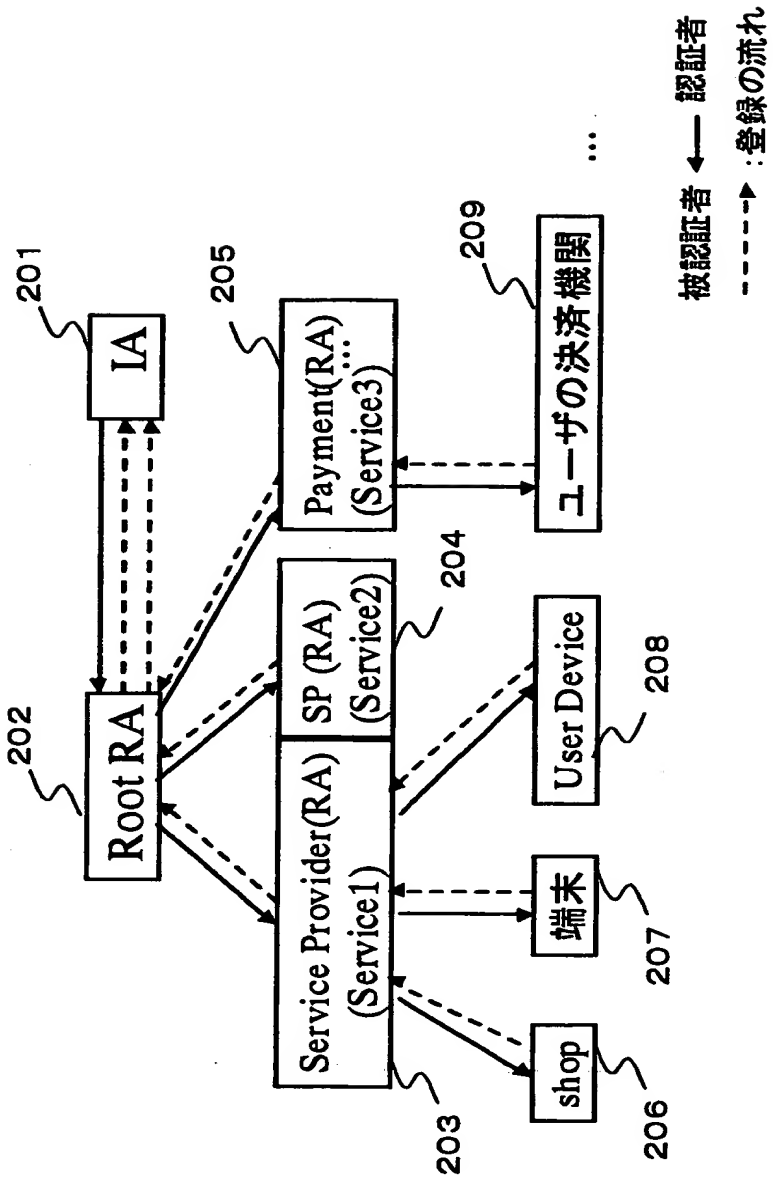
２２０１，２２０２　デバイス

【書類名】　　図面

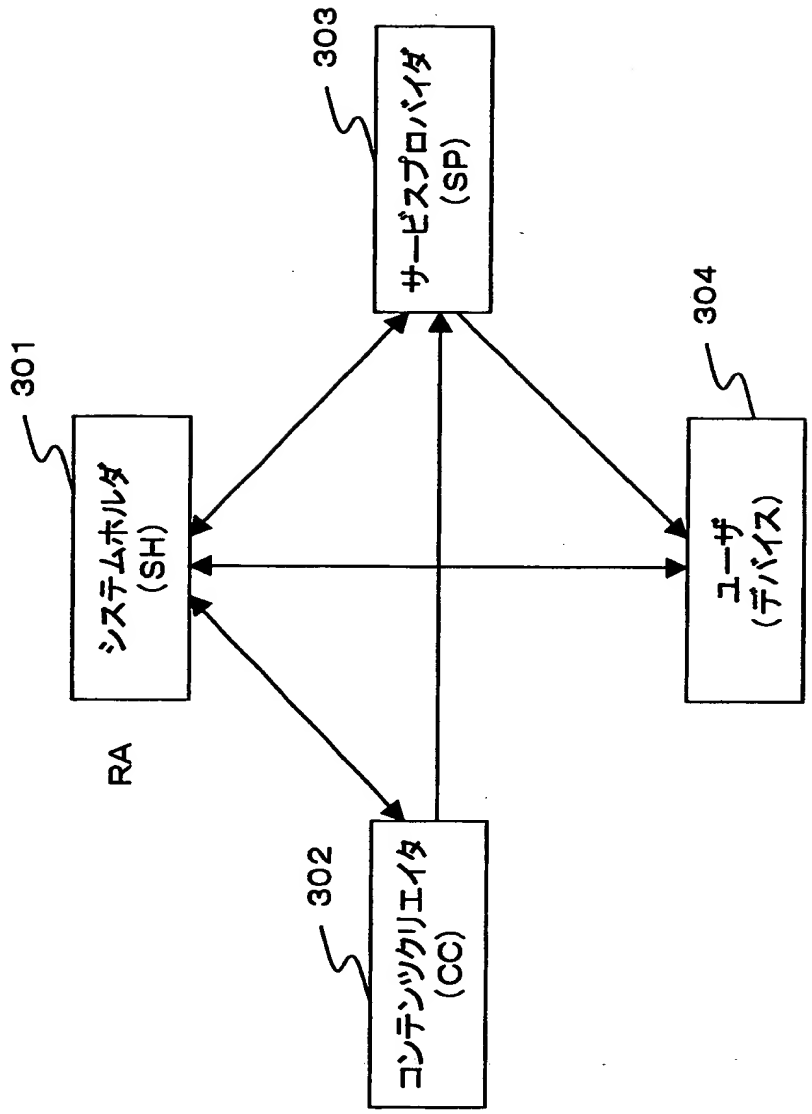
【図１】


メッセージ全体
電子署名
公開鍵証明書
証明書のバージョン番号
IAが割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
IAの名前
証明書の有効期限
証明書利用者の名前(ID)
証明書利用者の公開鍵
IAの秘密鍵
ハッシュ関数
メッセージ全体
公開鍵証明書

【図２】


201
IA
202
Root RA
205
Payment(RA)
(Service3)
204
SP (RA)
(Service2)
Service Provider(RA)
(Service1)
203
209
ユーザの決済機関
208
User Device
207
端末
206
shop
被認証者 ← 認証者
:登録の流れ

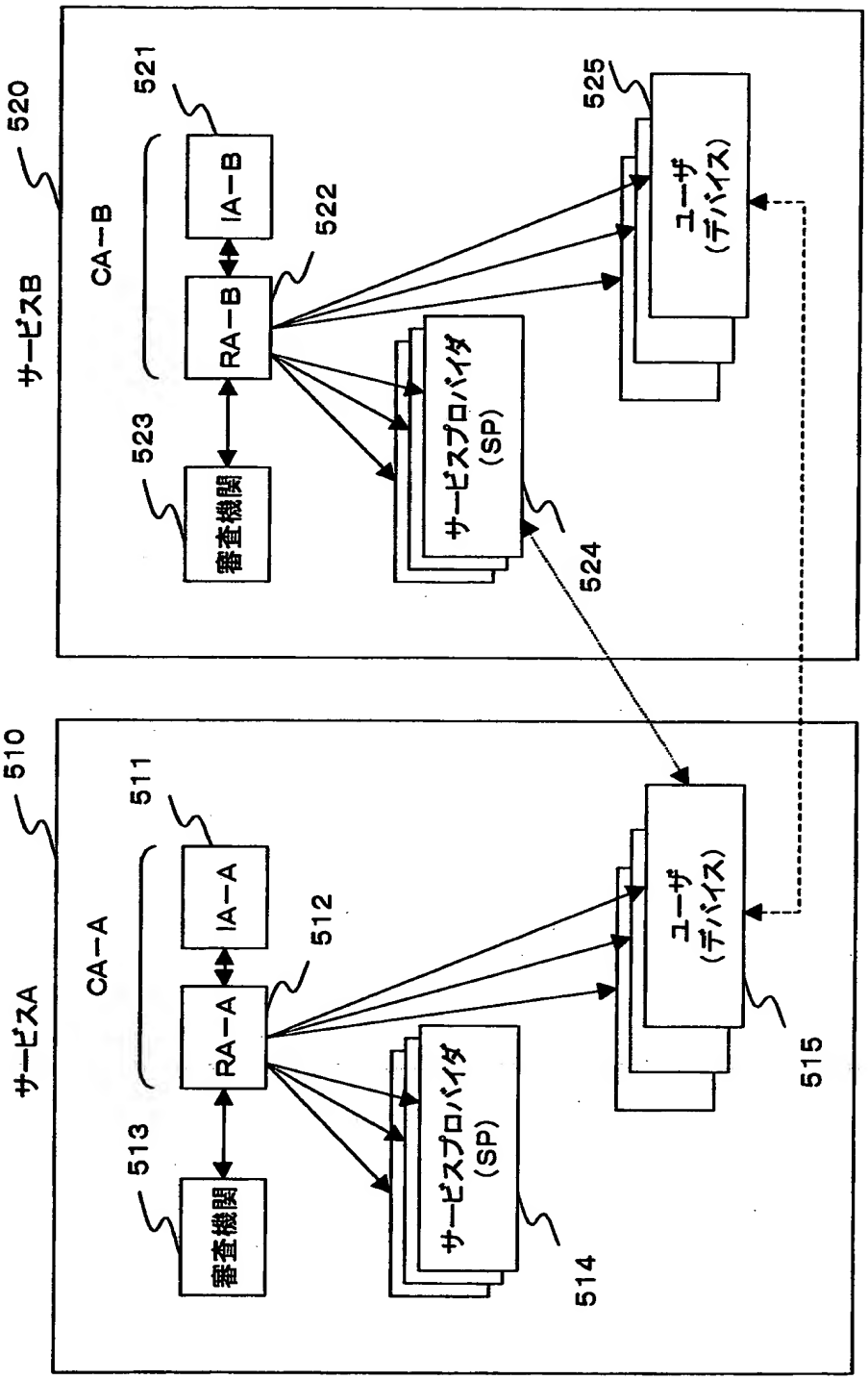
【図３】


303
サービスプロバイダ
(SP)
304
301
システムホルダ
(SH)
ユーザ
(デバイス)
RA
302
コンテンツクリエイタ
(CC)

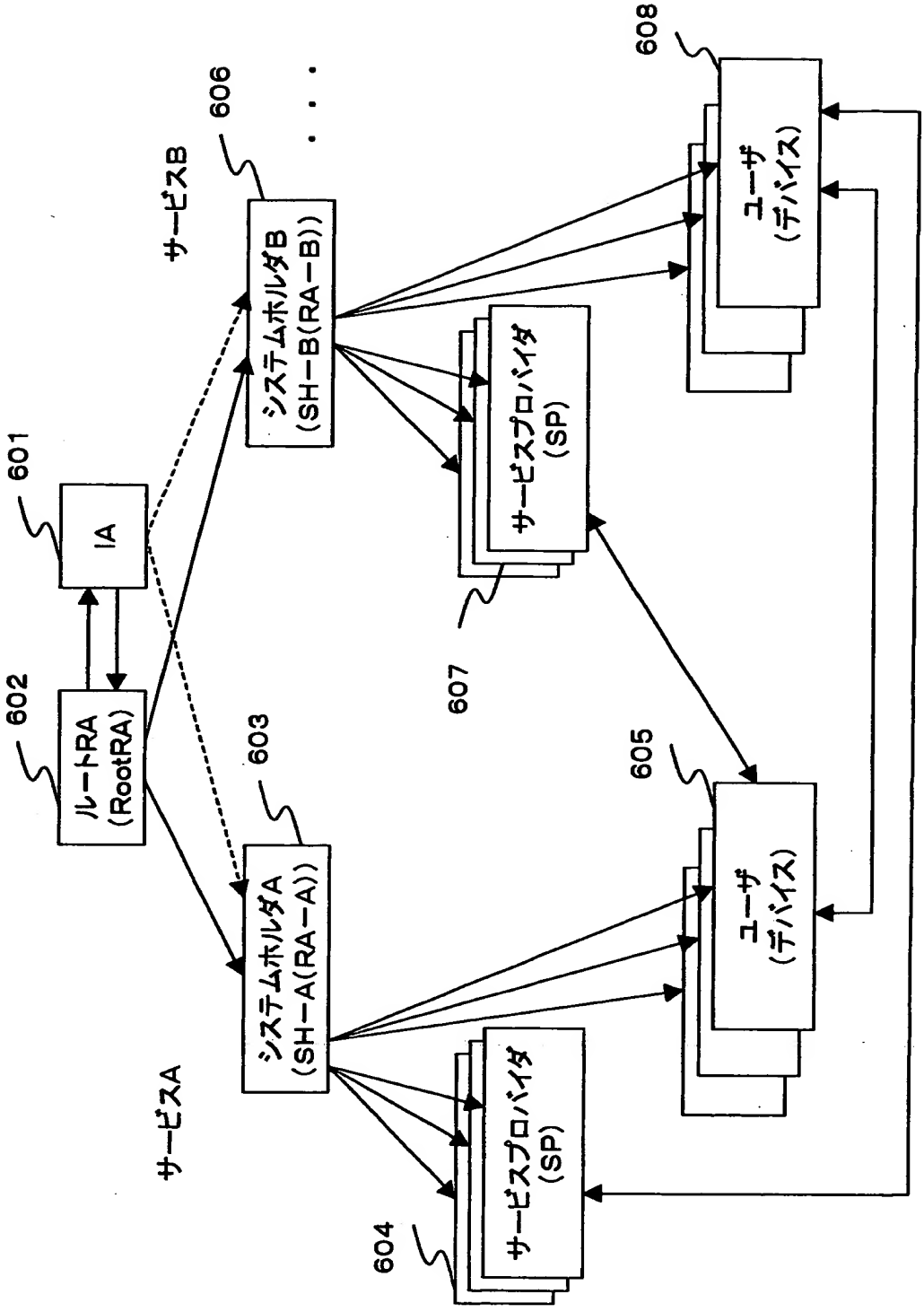
【図４】

No.	システムホルダ(SH)	コンテンツ・クリエイタ(CC)	サービスプロバイダ(SP)	ユーザデバイス
1.	インターネットショップ マーケット主催機関	マーケット提供商品、 コンテンツの生成、製造者	マーケット提供商品ショップ	PC
2.	携帯電話通信インフラ 提供機関	携帯電話インフラを利用した 提供コンテンツ、商品の生成者	携帯電話利用ユーザに対する コンテンツ配信者	携帯電話
3.	ケーブルテレビ ケーブル管理機関	ケーブルTV番組制作者	ケーブルTV会社	TV(受像機)
4.	電子マネー・カード 発行機関	電子マネーにより購入可能な 商品、コンテンツの生成者	電子マネー利用可能ショップ	ICカード
5.	：	：	：	：
6.	：	：	：	：

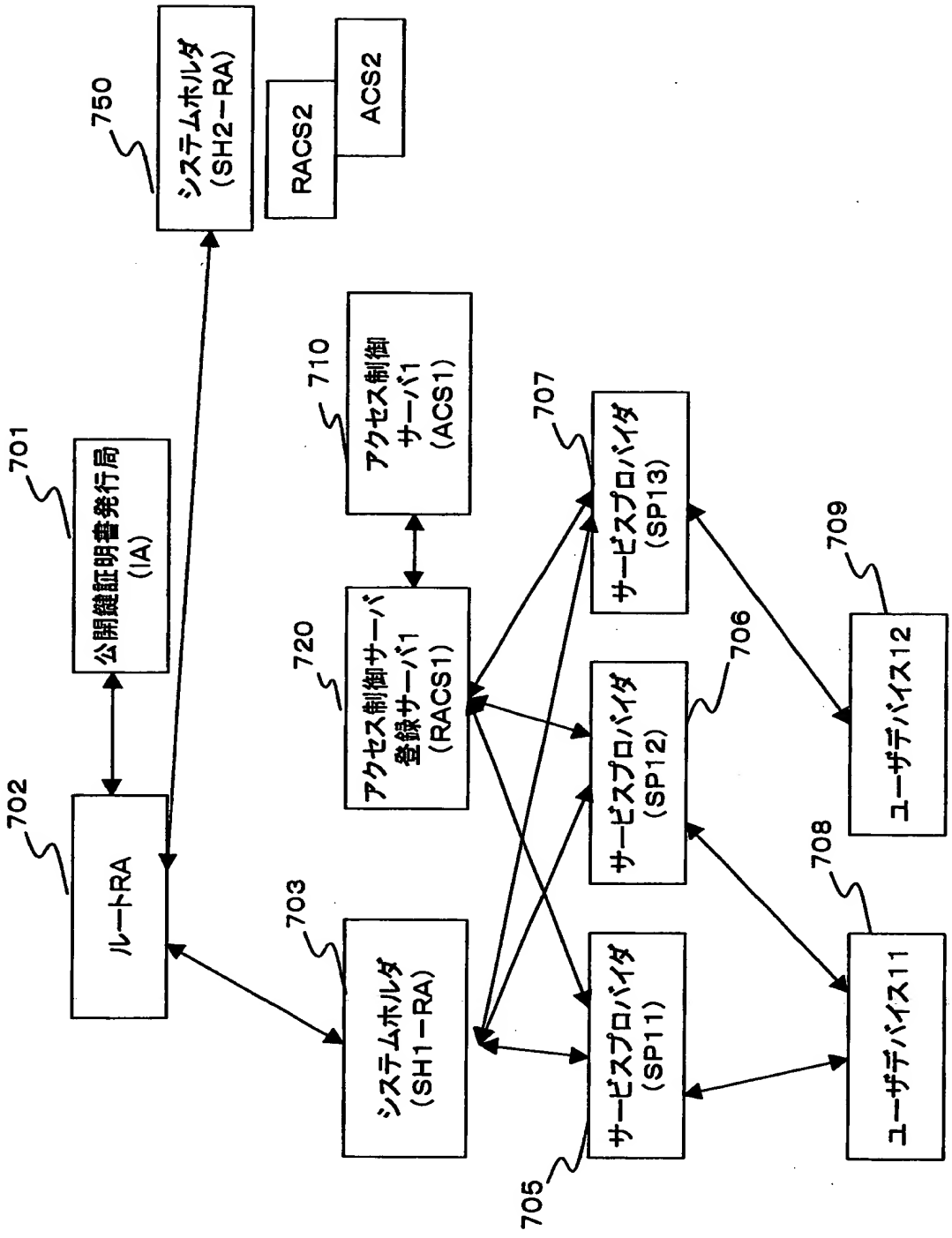
【図５】


サービスB
520
CA−B
521
IA−B
522
RA−B
523
審査機関
サービスプロバイダ
(SP)
524
525
ユーザ
(デバイス)
サービスA
510
CA−A
511
IA−A
512
RA−A
513
審査機関
サービスプロバイダ
(SP)
514
515
ユーザ
(デバイス)

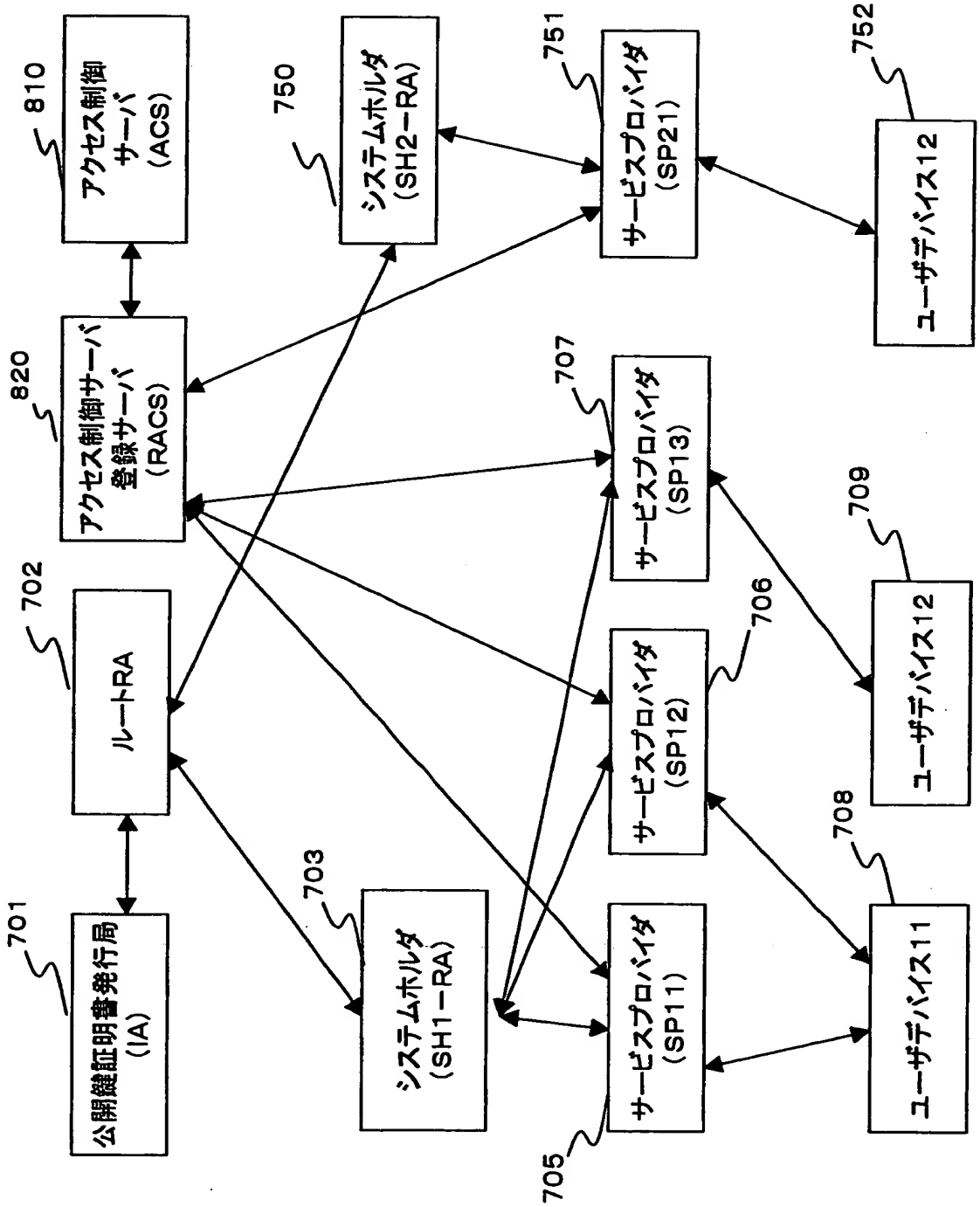
【図６】


608
606
サービスB
システムホルダB
(SH−B(RA−B))
ユーザ
(デバイス)
601
IA
サービスプロバイダ
(SP)
602
ルートRA
(RootRA)
607
603
605
システムホルダA
(SH−A(RA−A))
ユーザ
(デバイス)
サービスA
604
サービスプロバイダ
(SP)

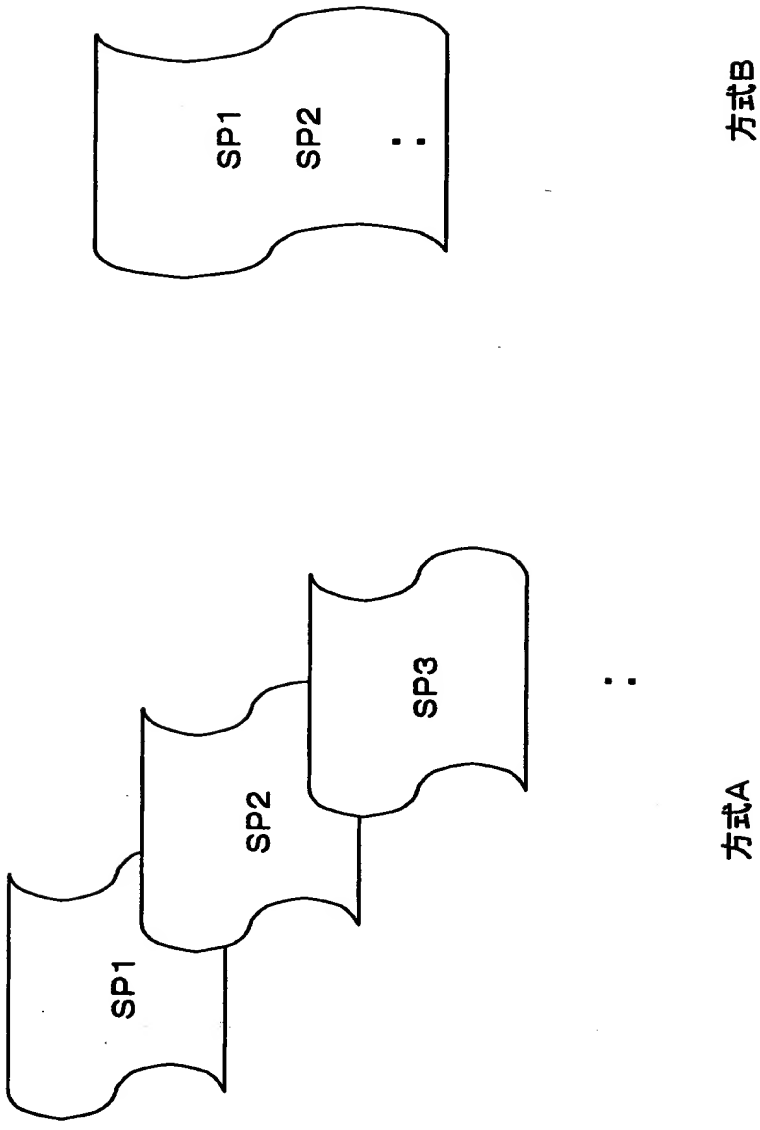
【図７】


システムホルダ
(SH2－RA)
RACS2
ACS2
750
公開鍵証明書発行局
(IA)
701
ルートRA
702
システムホルダ
(SH1－RA)
703
アクセス制御
サーバ1
(ACS1)
710
アクセス制御サーバ
登録サーバ1
(RACS1)
720
サービスプロバイダ
(SP13)
707
サービスプロバイダ
(SP12)
706
サービスプロバイダ
(SP11)
705
ユーザデバイス12
709
ユーザデバイス11
708

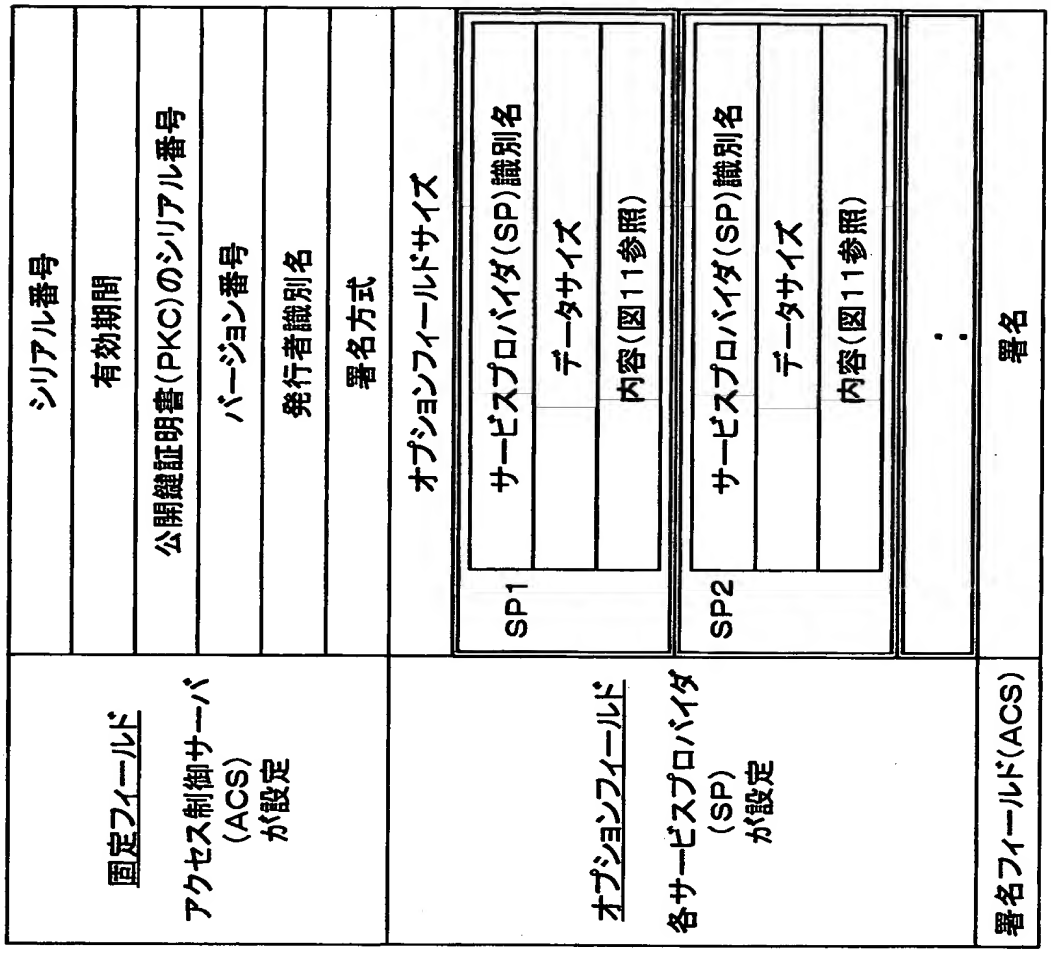
【図８】


公開鍵証明書発行局
(IA)
701
ルートRA
702
アクセス制御
サーバ
(ACS)
810
アクセス制御サーバ
登録サーバ
(RACS)
820
システムホルダ
(SH1－RA)
703
システムホルダ
(SH2－RA)
750
サービスプロバイダ
(SP11)
705
サービスプロバイダ
(SP12)
706
サービスプロバイダ
(SP13)
707
サービスプロバイダ
(SP21)
751
ユーザデバイス11
708
ユーザデバイス12
709
ユーザデバイス12
752

【図９】

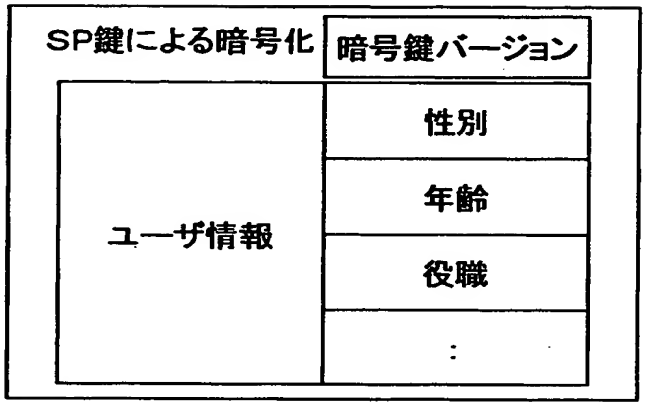


【図１０】

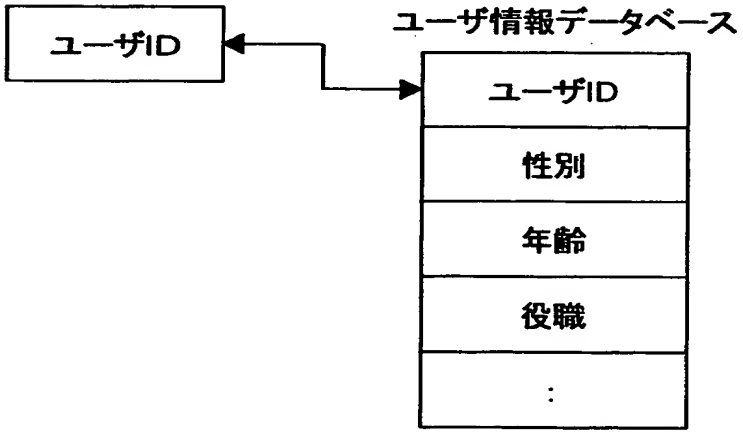

固定フィールド
アクセス制御サーバ(ACS)が設定
シリアル番号
有効期間
公開鍵証明書(PKC)のシリアル番号
バージョン番号
発行者識別名
署名方式
オプションフィールドサイズ
オプションフィールド
各サービスプロバイダ(SP)が設定
SP1
サービスプロバイダ(SP)識別名
データサイズ
内容(図11参照)
SP2
サービスプロバイダ(SP)識別名
データサイズ
内容(図11参照)
署名フィールド(ACS)
署名

【図１１】

方式イ）

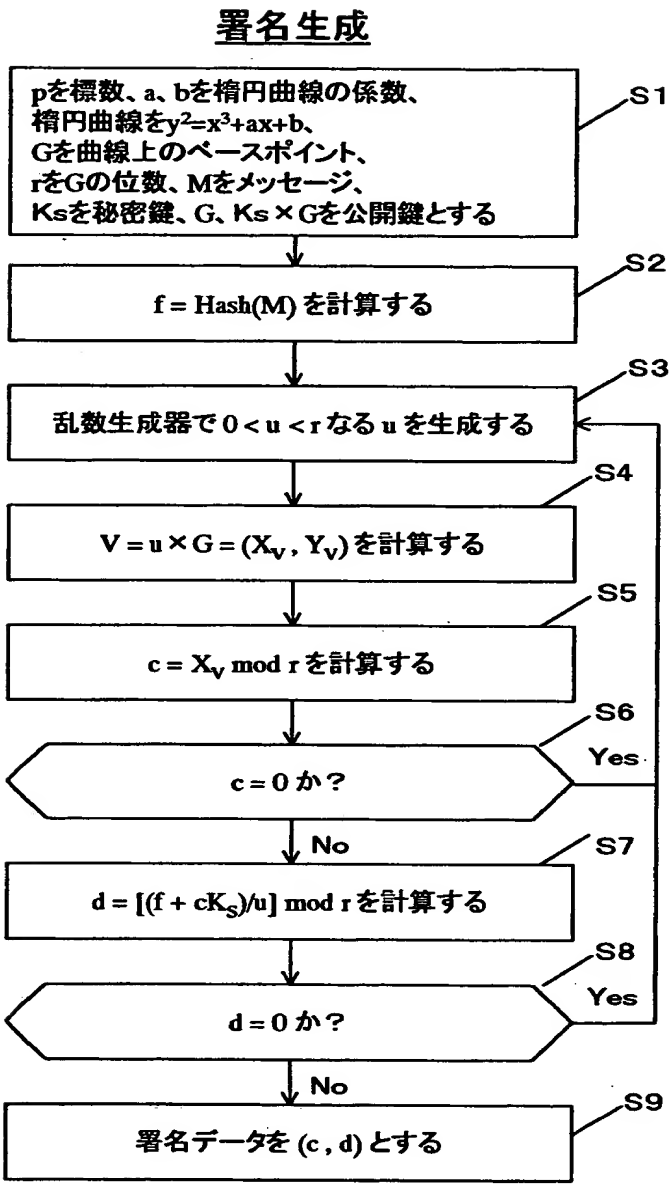


方式ロ）



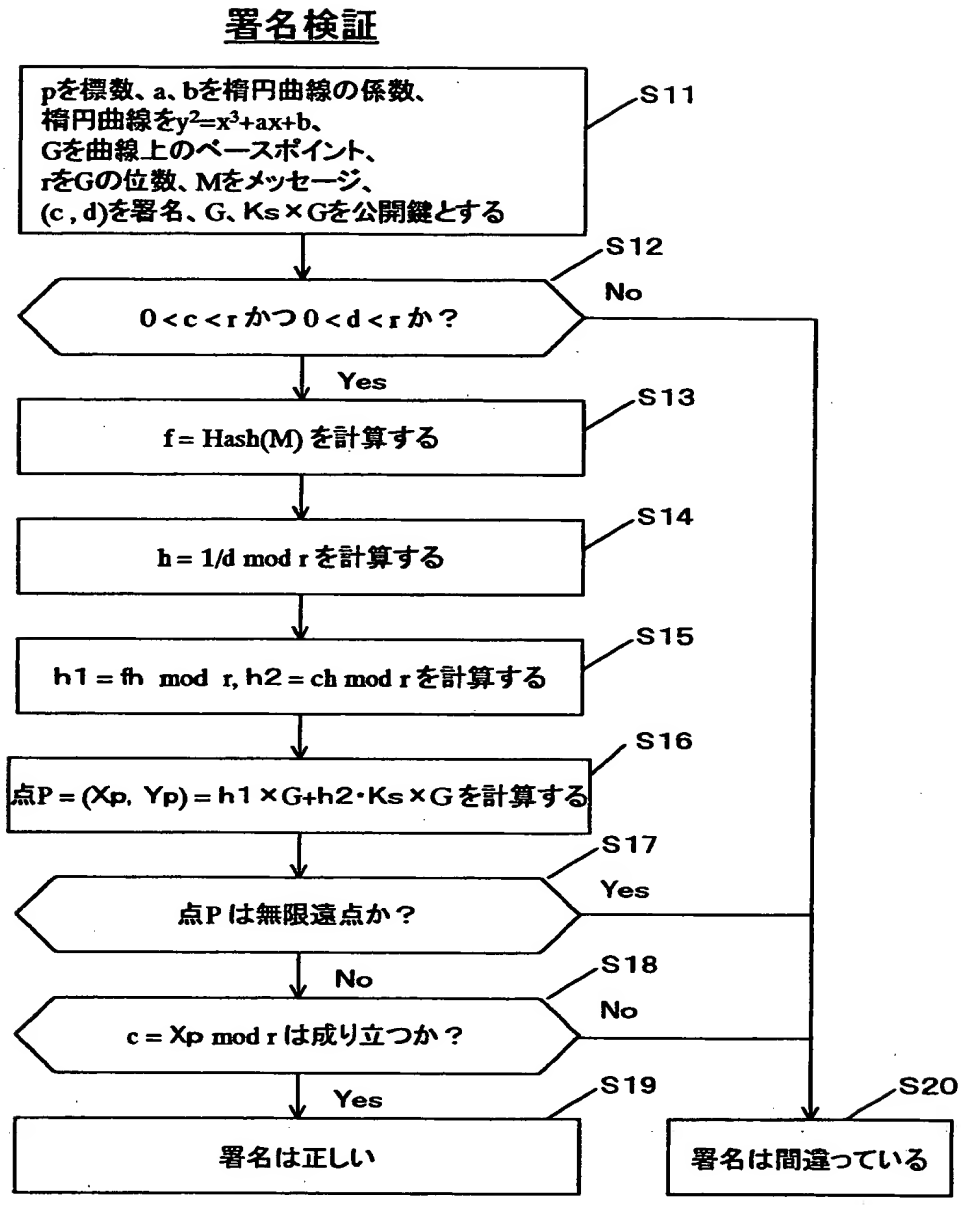
方式ハ）

【図１２】



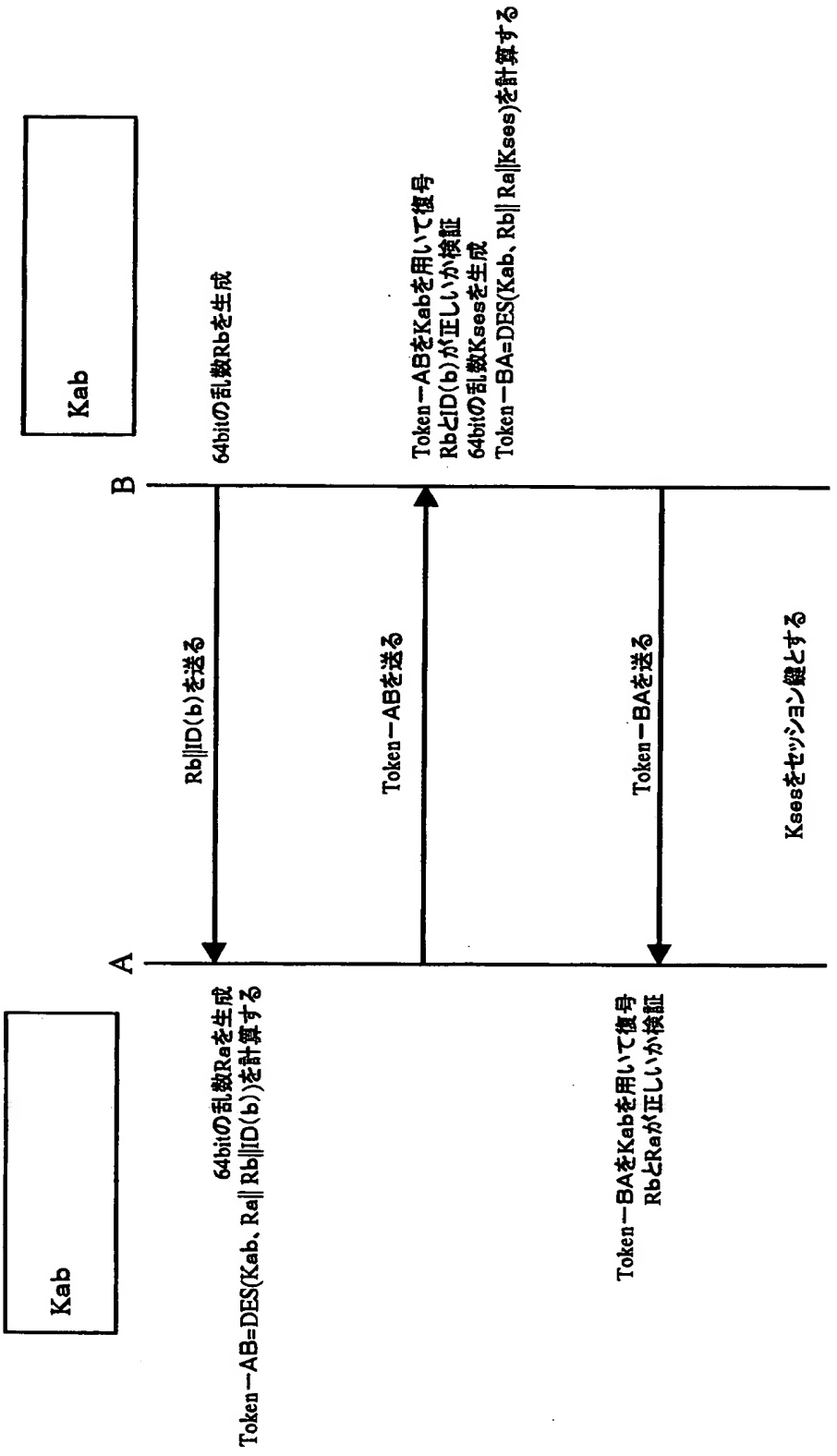
署名生成（IEEE P1363/D3）

【図１３】



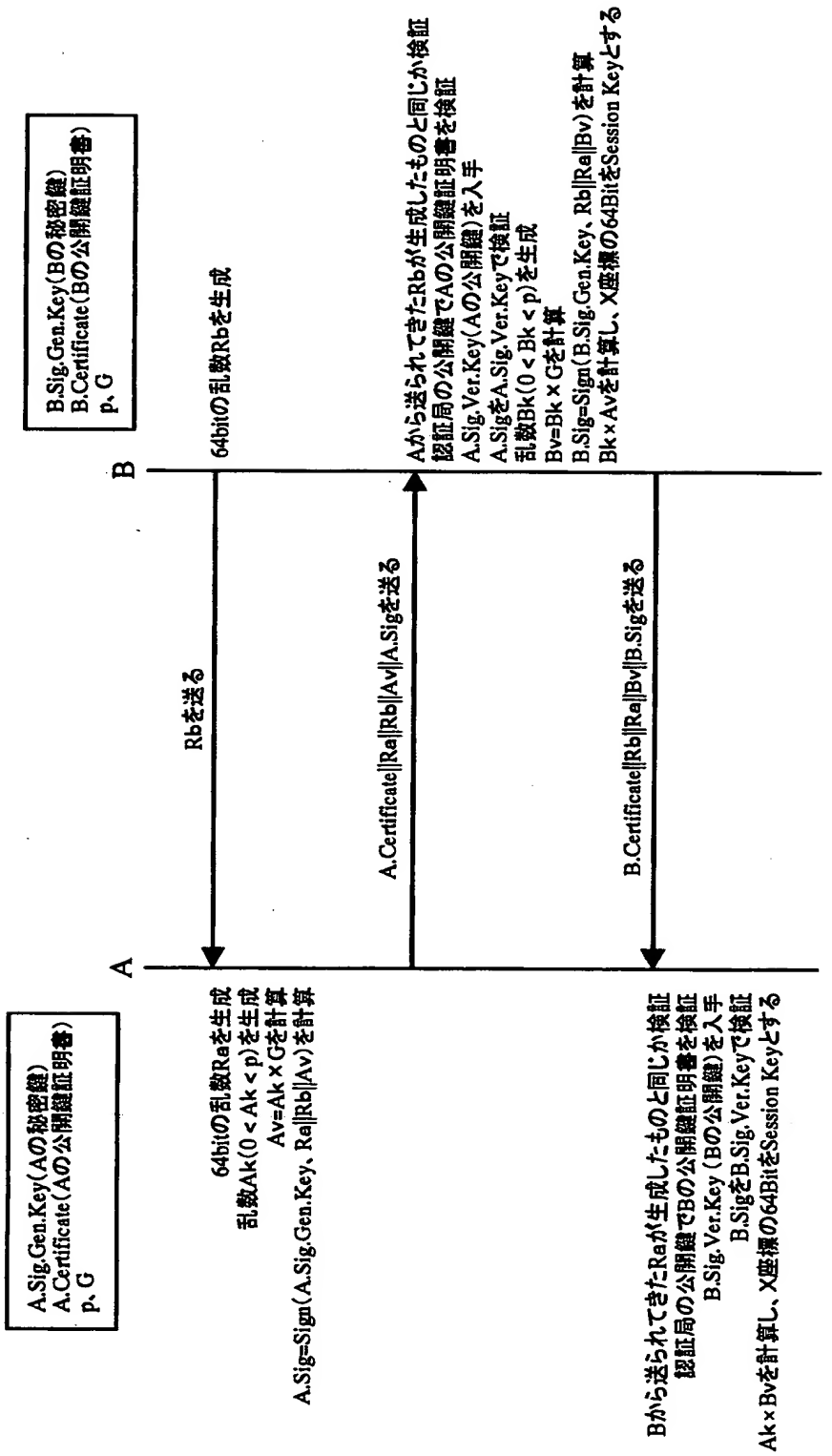
署名検証（IEEE P1363/D3）

【図１４】



ISO/IEC 9798-2　対称鍵暗号技術を用いた相互認証および鍵共有方式

【図１５】



ISO/IEC 9798-3　非対称鍵暗号技術を用いた相互認証および鍵共有方式

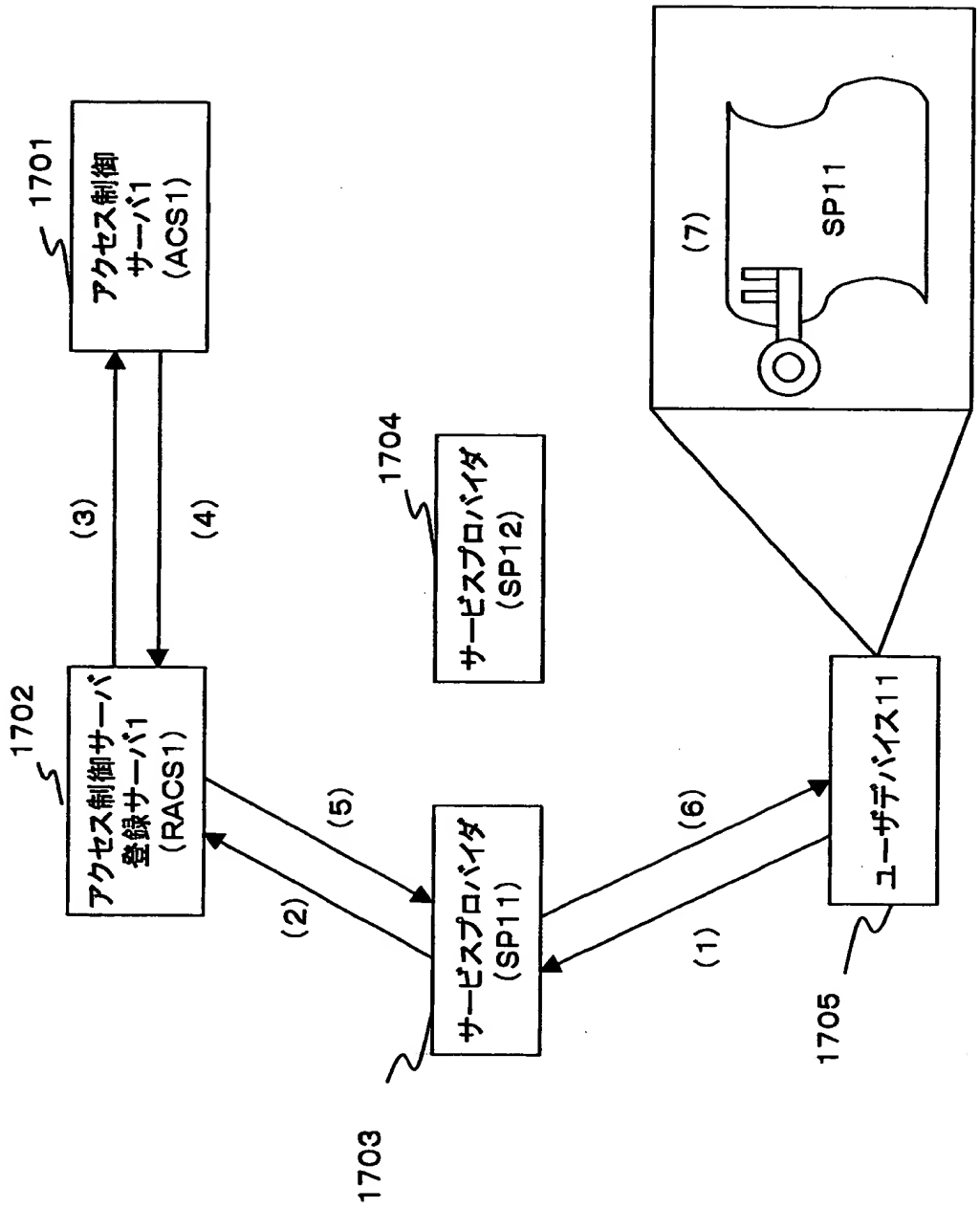
【図１６】

No.	用語	記号	説明・備考
1	公開鍵	K_{Pa}	Aの公開鍵。 例　User → K_{Pu}　UD → K_{Pud} SP → K_{Psp}
2	秘密鍵	K_{Sa}	Aの秘密鍵。 例　User → K_{Su}　UD → K_{Sud} SP → K_{Ssp}
3	セッション鍵	Ks	相互認証の際、作成される共通鍵
4	証明書	A《B》	Aが発行したBの証明書。 例：IAによるUDの証明書　→ IA《UD》
5	暗号化	E_{Ks}(data)	平文Dataを鍵Ksで暗号化
6	復号	D_{Ks}(data)	暗号文dataを鍵Ksで復号
7	署名	{data}Sig.K_{Sa}	DataをAの秘密鍵K_{Sa}で署名
8	署名付き暗号化	E_{Ks}({data}Sig.K_{Sa})	dataをAの秘密K_{Sa}で署名し，(data‖署名)を鍵Ksで暗号化

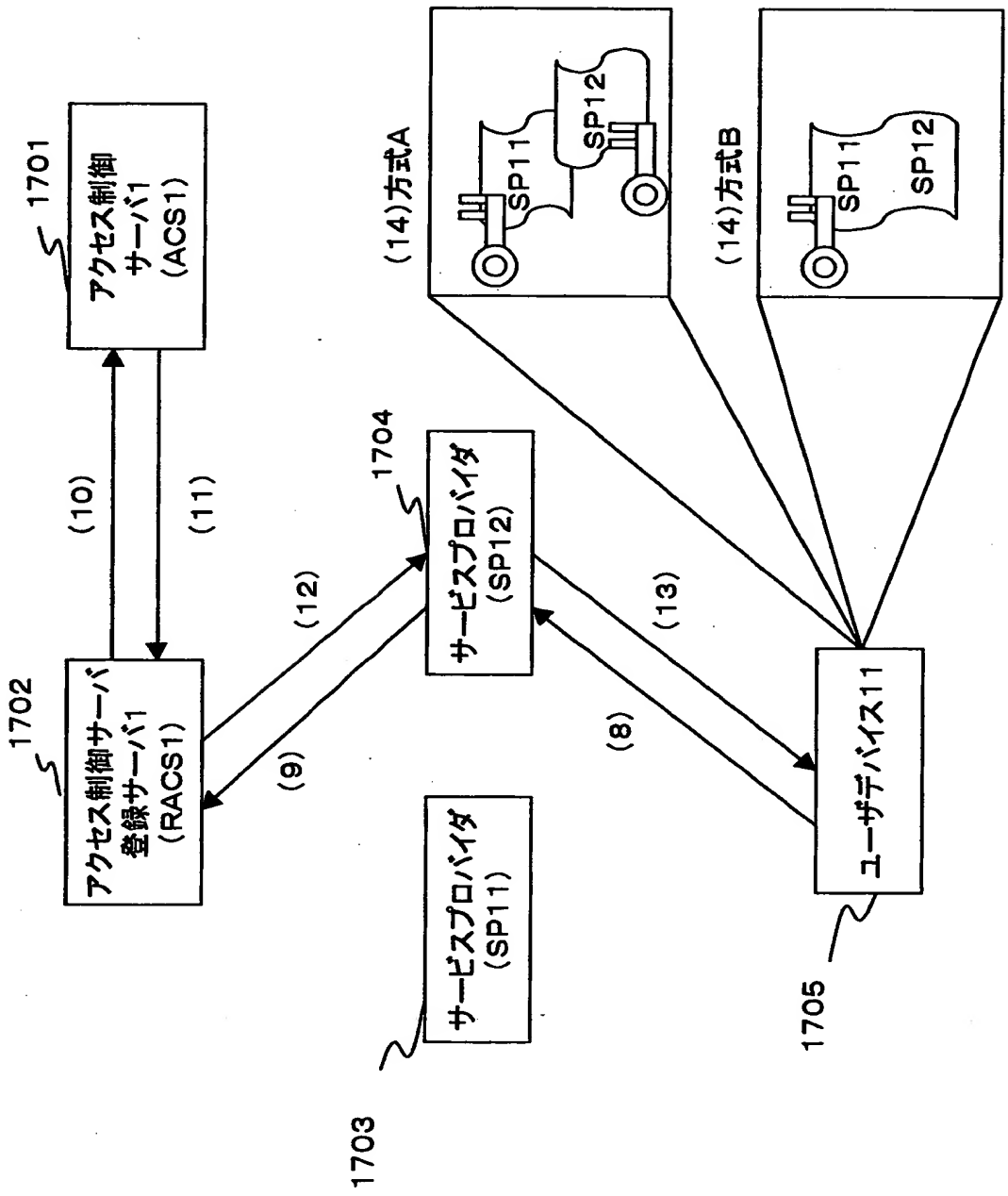
出証特２００１－３０１６４３９

特２０００－１２５７８７

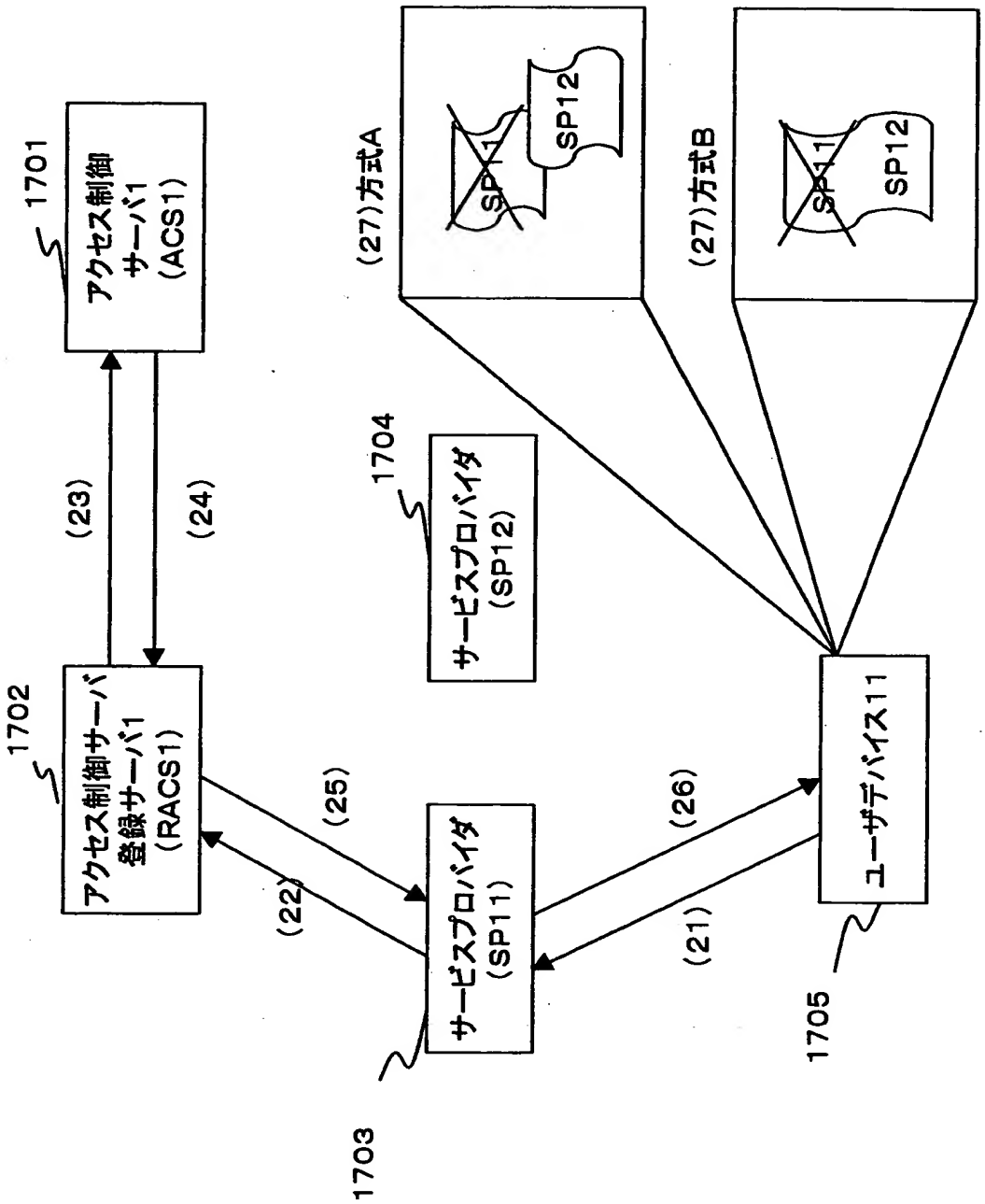
【図１７】


1701
アクセス制御
サーバ1
(ACS1)
(3)
(4)
1702
アクセス制御サーバ
登録サーバ1
(RACS1)
1704
サービスプロバイダ
(SP12)
(5)
(2)
サービスプロバイダ
(SP11)
1703
(6)
(1)
ユーザデバイス11
1705
(7)
SP11

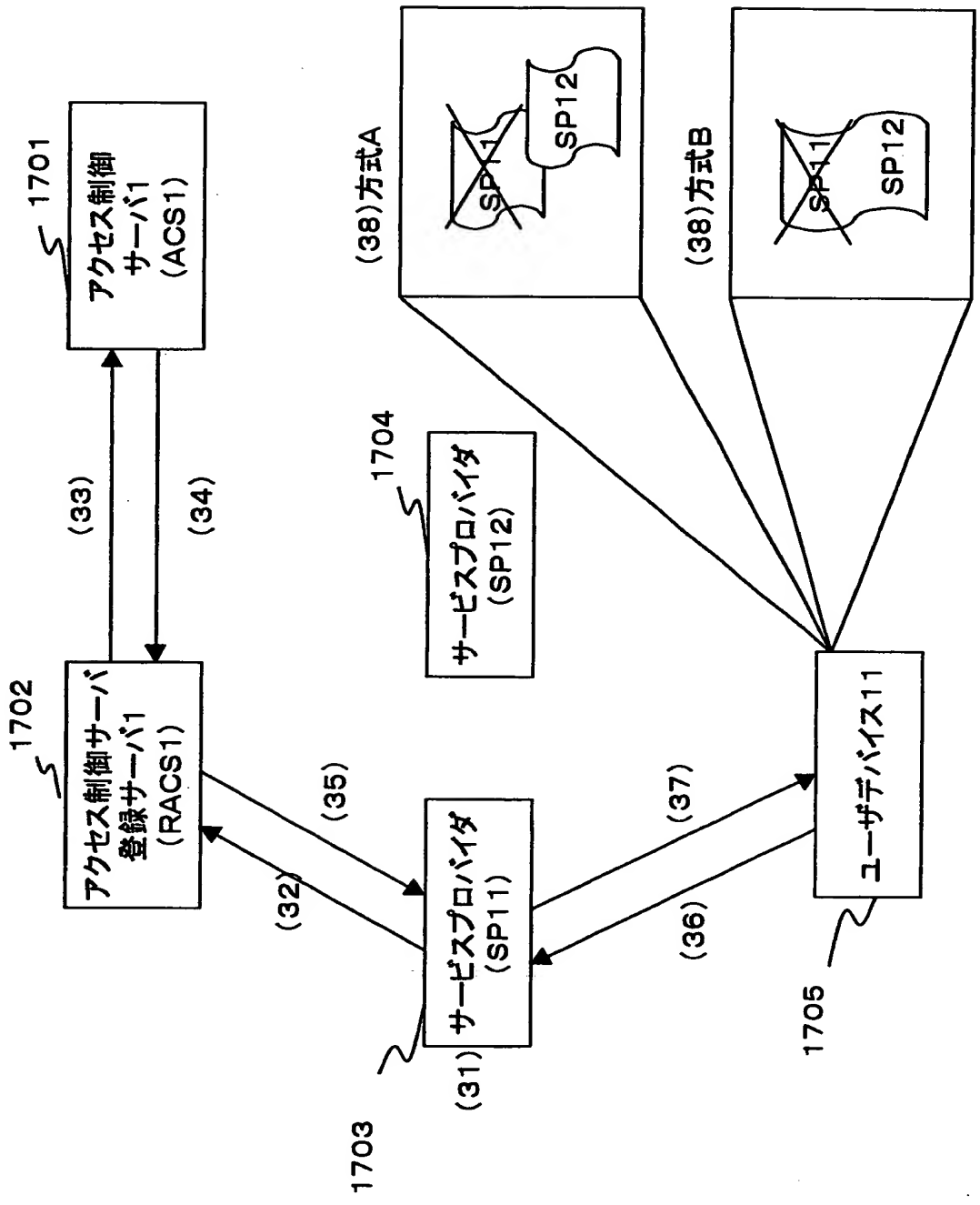
【図１８】


アクセス制御
サーバ1
(ACS1)
1701
アクセス制御サーバ
登録サーバ1
(RACS1)
1702
サービスプロバイダ
(SP11)
1703
サービスプロバイダ
(SP12)
1704
ユーザデバイス11
1705
(8)
(9)
(10)
(11)
(12)
(13)
(14)方式A
(14)方式B
SP11
SP12

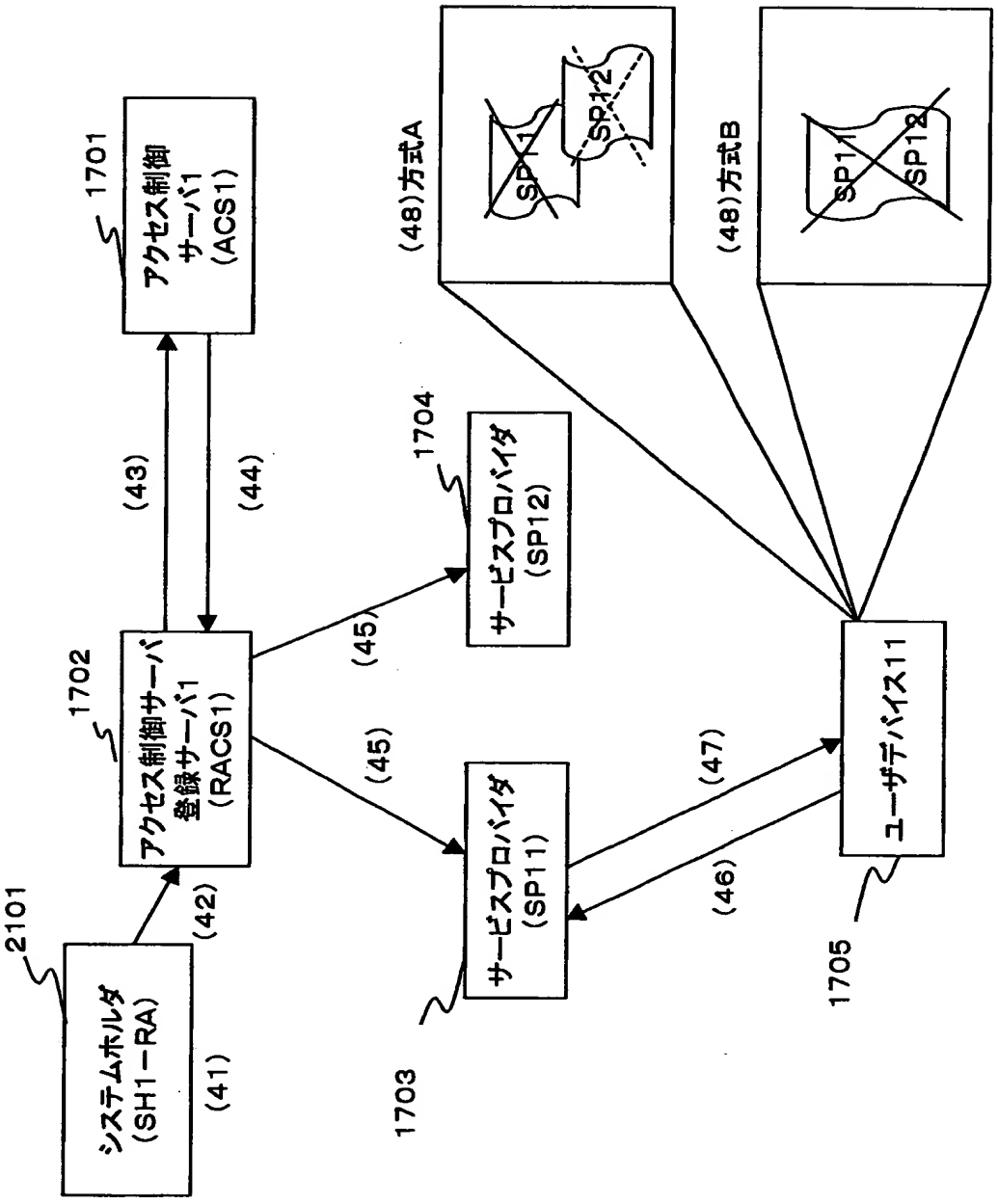
【図１９】


アクセス制御
サーバ1
(ACS1)
1701
(23)
(24)
アクセス制御サーバ
登録サーバ1
(RACS1)
1702
(25)
(22)
サービスプロバイダ
(SP11)
1703
(26)
(21)
ユーザデバイス11
1705
サービスプロバイダ
(SP12)
1704
(27)方式A
SP11
SP12
(27)方式B
SP11
SP12

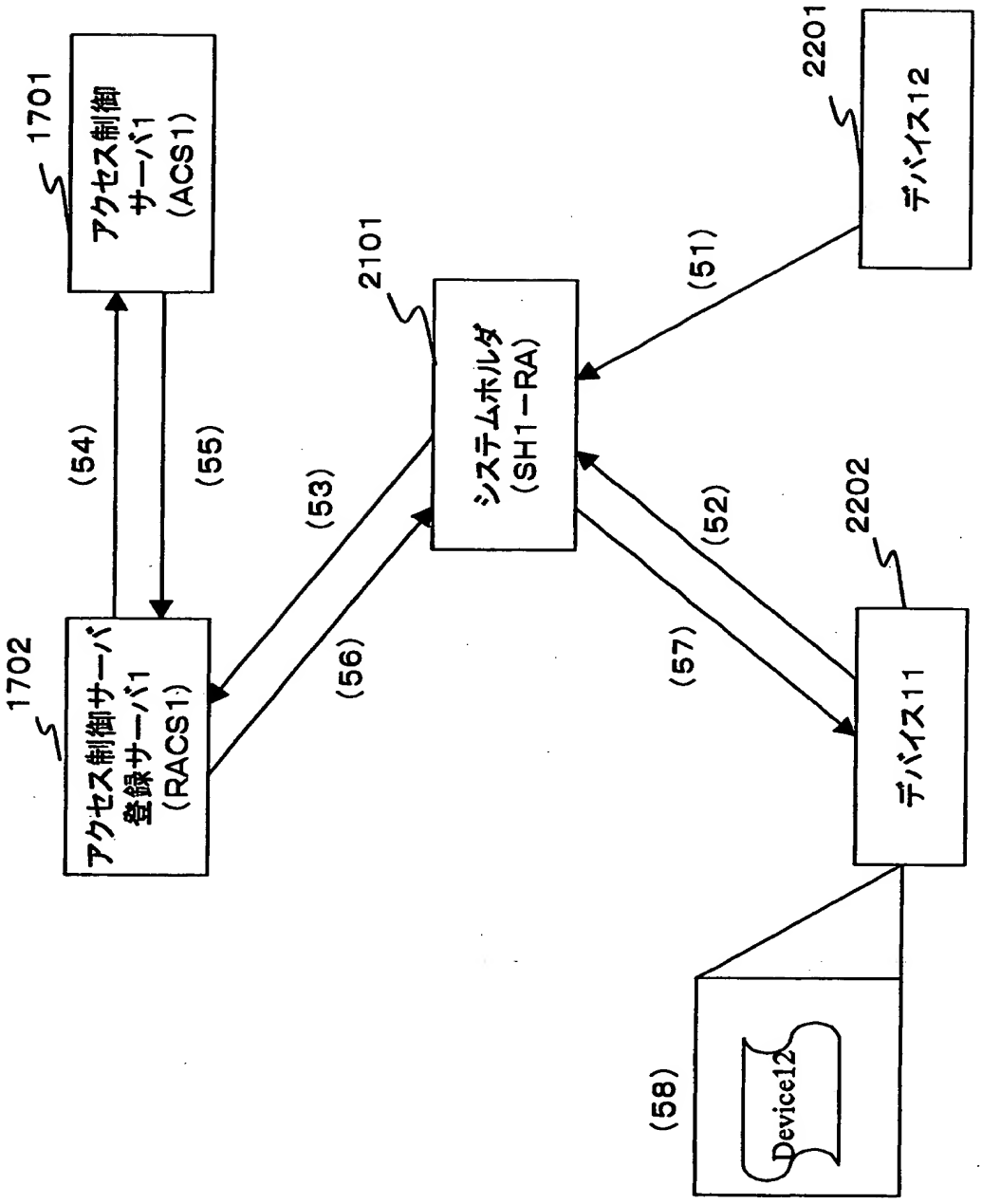
【図２０】


アクセス制御
サーバ1
(ACS1)
1701
(33)
(34)
アクセス制御サーバ
登録サーバ1
(RACS1)
1702
(35)
(32)
サービスプロバイダ
(SP11)
(31)
1703
1704
サービスプロバイダ
(SP12)
(37)
(36)
ユーザデバイス11
1705
(38)方式A
SP11
SP12
(38)方式B
SP11
SP12

【図２１】


システムホルダ
(SH1－RA)
2101
(41)
(42)
アクセス制御サーバ
登録サーバ1
(RACS1)
1702
(43)
(44)
アクセス制御
サーバ1
(ACS1)
1701
(45)
(45)
サービスプロバイダ
(SP12)
1704
サービスプロバイダ
(SP11)
1703
(47)
(46)
ユーザデバイス11
1705
(48)方式A
SP11
SP12
(48)方式B
SP11
SP12

【図２２】


1701
アクセス制御
サーバ1
(ACS1)
2201
デバイス12
2101
システムホルダ
(SH1－RA)
(51)
(54)
(55)
(53)
(52)
2202
1702
アクセス制御サーバ
登録サーバ1
(RACS1)
(56)
(57)
デバイス11
(58)
Device12

【書類名】　　要約書

【要約】

【課題】　サービスプロバイダが個々にアクセス制御を行なうことを不要としたアクセス制御システムを提供する。

【解決手段】　複数のサービスプロバイダ、デバイスに共通に利用されるアクセス制御サーバが設置され、アクセス制御サーバが規定するフォーマット、手順に従ったアクセス許可書を発行する。アクセス許可書に従ってアクセス制御が実行され、各サービスプロバイダ、デバイスは、独自のアクセス制御手順を構築することなく、容易にアクセス制御を実行することが可能となる。サービスを受けるユーザデバイスにおいても個々のサービスプロバイダに応じたアクセス処理シーケンスを実行することなく、一定シーケンスに従った処理が可能となるので、サービスプロバイダ毎のフォーマットデータ、アクセスプログラム等を個別に格納管理する必要がない。

【選択図】　図７

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社